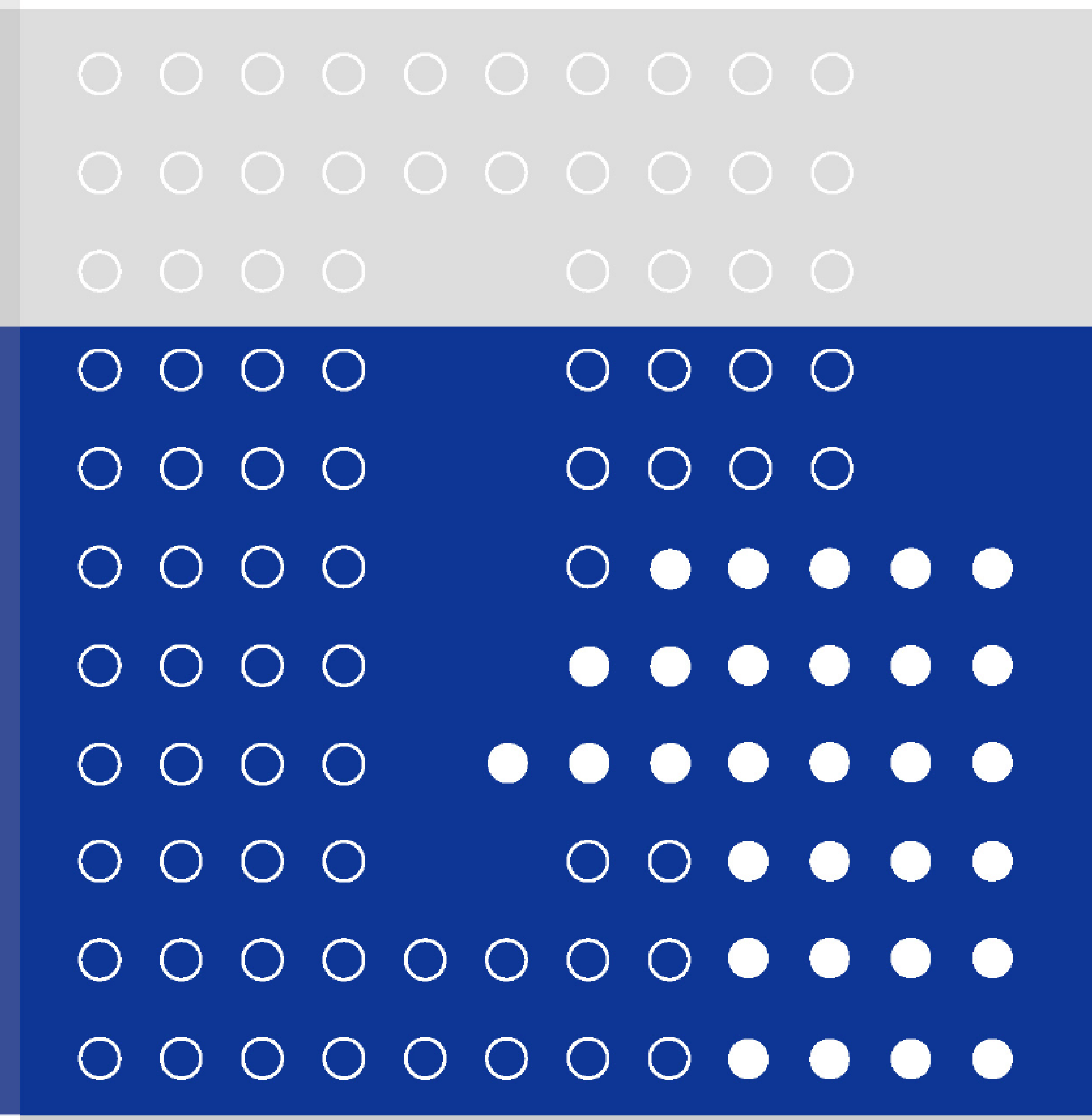


普通高等教育“十一五”国家级规划教材　计算机系列教材

教育部信息安全特色专业建设项目

网络安全协议



赖英旭　杨震　刘静　编著

李健　审

清华大学出版社

计算机系列教材
教育部信息安全特色专业建设项目

网络安全协议

赖英旭　杨　震　刘　静　编著
李　健　审

清华大学出版社
北　京

内 容 简 介

本书比较全面地介绍了网络安全协议的关键技术和主要应用模式。特别对 VPN 网络的特点、分类及应用模式等方面进行了比较深入的分析和探讨。

本书对数据链路层安全协议、网络层安全协议、传输层安全协议、会话层安全协议和应用层安全协议等方面进行了比较深入的分析，并介绍了各层协议的安全缺陷、易受到的攻击以及在相应层协议中所增强的安全机制。在网络安全协议应用方面，本书重点阐述了 3 种常见的 VPN 网络应用模式，并比较详细地介绍了 VPN 网络的工作原理和配置。

本书通俗易懂，注重可操作性和实用性。通过对典型 VPN 网络应用模式案例的讲解，使读者能够举一反三。本书可作为广大计算机用户、计算机安全技术人员的技术参考书，特别是可用做信息安全、计算机与其他信息学科本科生的教材，也可用做计算机信息安全职业培训的教材。

图书在版编目 CIP 数据

网络安全协议/赖英旭，杨震，刘静编著. —北京：清华大学出版社，2012.10
（计算机系列教材）
ISBN 978-7-302-27903-7

Ⅰ. ①网…　Ⅱ. ①赖…　②杨…　③刘…　Ⅲ. ①计算机网络—安全技术—通信协议—高等学校—教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 008916 号

责任编辑：汪汉友
封面设计：常雪影
责任校对：梁　毅
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**15.5　　**字　　数：**370 千字
版　　次：2012 年 10 月第 1 版　　**印　　次：**2012 年 10 月第 1 次印刷
印　　数：1～3000
定　　价：26.00 元

产品编号：035509-01

前 言

网络安全一直是一个倍受关注的领域。如果缺乏一定的安全保障，无论是公共网络还是企业专用网络，都难以抵挡网络攻击和非法入侵。如果没有适当的安全措施和访问控制方法，在网络上传输的数据很容易受到各式各样的攻击。本书主要介绍从数据链路层到应用层，安全协议在保证数据传输安全性方面所采取的关键技术。

本书由北京工业大学从事教育部"信息安全"特色专业建设的教师编写（从事大学本科网络安全协议教学6年、研发工作6年）。书中重点分析了网络安全协议的运行机制，并采用大量案例讲解安全协议的应用。

本书分为9章，具体内容如下。

第1章　安全标准。介绍国内外主要的安全评价标准，重点介绍国际上通用的信息技术安全性评价通用准则(CC)，并通过介绍流行操作系统的等级，使读者更加清晰地了解信息技术安全性评价通用准则的使用。

第2章　数据链路层安全协议。本章首先介绍了原有数据链路层协议的安全问题，为了增强数据链路层协议的安全性，着重介绍了局域网数据链路层安全协议 IEEE 802.10 和 IEEE 802.1q、广域网数据链路层安全协议 L2TF 和 PPTP 以及无线网数据链路层安全协议 IEEE 802.11 和 IEEE 802.1x。

第3章　网络层安全协议。本章介绍网络攻击的特点及危害和工作原理等。为了让读者更充分了解网络层安全协议的技术特征，又详细地介绍网络安全协议 IPSec 的体系结构，IPSec 所包含的安全协议、安全联盟和密钥交换等关键技术。

第4章　传输层安全协议。本章详细分析传输层安全协议 SSL 的握手协议和记录协议。此外，还对 SSL 的安全性进行了分析。

第5章　会话层安全协议。本章介绍会话层安全协议 SSH 的主要安全机制、SSH 身份认证协议和 SSH 连接协议。为了使读者对 SSH 协议的应用理解得更加深入，还对 SSH 的典型应用案例进行了介绍。

第6章　应用层安全协议。本章介绍安全电子邮件协议和 S-HTTP 协议，使读者了解为了降低应用层协议受到的攻击，在应用层安全协议中所采用的安全机制。

第7章　VPN 基础。本章介绍安全协议最重要的应用——构建 VPN 网络，内容包括 VPN 的工作原理、特点和分类。重点讲述了 VPN 的3种应用模式：构建企业内部虚拟网络、构建企业外部虚拟网络和远程接入虚拟网络。

第8章　VPN 应用案例。本章通过 A 公司和某高校网络两个案例，介绍3种 VPN

应用模式的配置要点，为构建安全网络体系提供解决方案。

第 9 章　VPN 产品介绍和选购标准。本章对国内外流行的 VPN 产品进行了介绍，给出各产品的技术特点，并在最后给出了公司构建虚拟专用网络(VPN)时的选购标准。

本书由北京工业大学赖英旭、杨震、刘静和杨胜志共同编写，其中第 1 章～第 3 章由赖英旭编写，第 4 章～第 6 章由杨震编写，第 7 章和第 9 章由刘静编写，第 8 章由杨胜志编写。全书最后由赖英旭和杨震统稿，李健审定。

本书的研究和编写工作受到教育部和北京市“信息安全特色专业建设项目”资助。本书从各种论文、图书、期刊以及互联网中引用了大量的文献资料，在文字的录入和整理中得到了李健老师的帮助，在此谨表示衷心感谢。

由于时间和水平有限，书中难免有误，恳请读者批评指正，使本书得以改进和完善。

作　者

2012 年 6 月

目 录

第1章 安全标准

为了对现有计算机系统的安全性进行统一评价，为计算机系统制造商提供一个权威的系统安全性标准，需要有一个计算机系统安全测评标准。美国国防部于1983年推出了历史上第一个计算机评价准则——《可信计算机系统评价准则》(TCSEC)，带动了国际上计算机安全测评的研究。随后，各国也相继发布了自己的信息安全技术标准：欧盟发布了信息技术安全评价标准(ITSEC)、加拿大发布了加拿大可信计算机产品评价标准(CTCPEC)、美国发布了信息技术安全联邦标准(FC)等。这些标准基本上都采用了TCSEC的安全框架和模式，将信息系统的安全性分成不同等级，并规定了不同等级应实现的安全功能或安全措施，它们之间的关系可用图1-1来表示。近年来，我国也制定了相应的强制性国家标准和推荐标准。

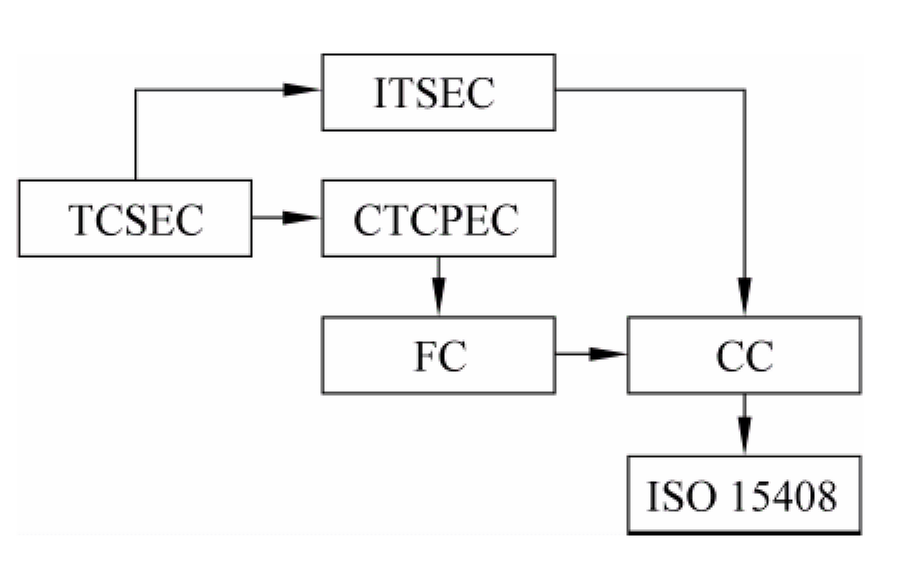


图1-1 评测标准关系图

下面列出了几个常用的安全标准。

(1) 美国TCSEC。美国国防部于1983年制定，提供D、C1、C2、B1、B2、B3、A1这7个等级的可信系统评价标准，每个等级对应有确定的安全特性需求和保障需求，高等级需求建立在低等级需求的基础之上。

(2) 欧洲ITSEC。1991年，西欧四国制定了信息技术安全评价规则(ITSEC)，ITSEC首次提出了信息安全的保密性、完整性和可用性概念，把可信计算基的概念提高到可信信息技术的高度上来认识。它定义了从E0～E6这7个安全等级和10种安全功能。

(3) 联邦标准FC。由美国国家标准与技术协会和国家安全局联合开发的拟用于取代TCSEC标准的计算机安全评价标准。该标准把安全功能和安全保证分离成两个独立的部分，并提出了保护轮廓定义书和安全目标定义书的概念。该标准只有草案，没有正式版本。

(4) 通用准则CC。1993年6月，美国、加拿大及欧洲4国经协商同意，起草单一的通用准则(CC)，并将其推进到国际标准。CC结合了FC及ITSEC的主要特征，它强调将安全的功能与保障分离，并将功能需求分为9类63族，将保障分为7类29族。

(5) GB 17859—1999。中国国家技术监督局参考TCSEC和可信计算机网络系统说明(NCCS)而制定的国家强制标准，共分5个安全等级。

(6) GB/T 18336—2001：中国国家技术监督局参考CC标准而制定的国家推荐标准，共分为3个部分：简介和一般模型、安全功能要求和安全保证要求。

1.1 国内外发展现状

1.1.1 TCSEC

1983年,美国国防部颁布了历史上第一个计算机安全评价标准,这就是著名的可信计算机系统评价标准,简称TCSEC,又称橙皮书。1985年,美国国防部对TCSEC进行了修订。

如图1-2所示,TCSEC定义了7个等级(D,C1,C2,B1,B2,B3,A1)组成的4个类别,类A中的级别A1是最高安全级别,类D中的级别D是最低安全级别。类别用来度量提供安全保护的程度,每一个级别和类别都是在前一个基础上增加条款形成的。TCSEC还给出了与安全政策、责任、保障和文档相关的两条明确可操作的评估准则,并给出了TCSEC的测试需求。TCSEC准则的原理是在C1级别设立基本安全要求,然后在高安全级别的每一层都加入新的需求。TCSEC引入了"可信计算机基(TCB)"和"安全内核(或引用监视器)"两个重要概念,TCB是硬件、固件和实施某项安全政策的软件的组合表示,是安全机制的抽象。"安全内核(或引用监视器)"是硬件、固件和软件的组合,该软件不仅实现访问控制功能,而且保护自己免受篡改。"安全内核"实现了系统安全政策的强制访问控制功能,是安全机制的具体实现。TCSEC要求安全模型A1级别的设计必须通过形式化的数学证明,形式化的安全模型在今天仍然具有重要性,形式化可用于安全系统的需求说明和设计验证。

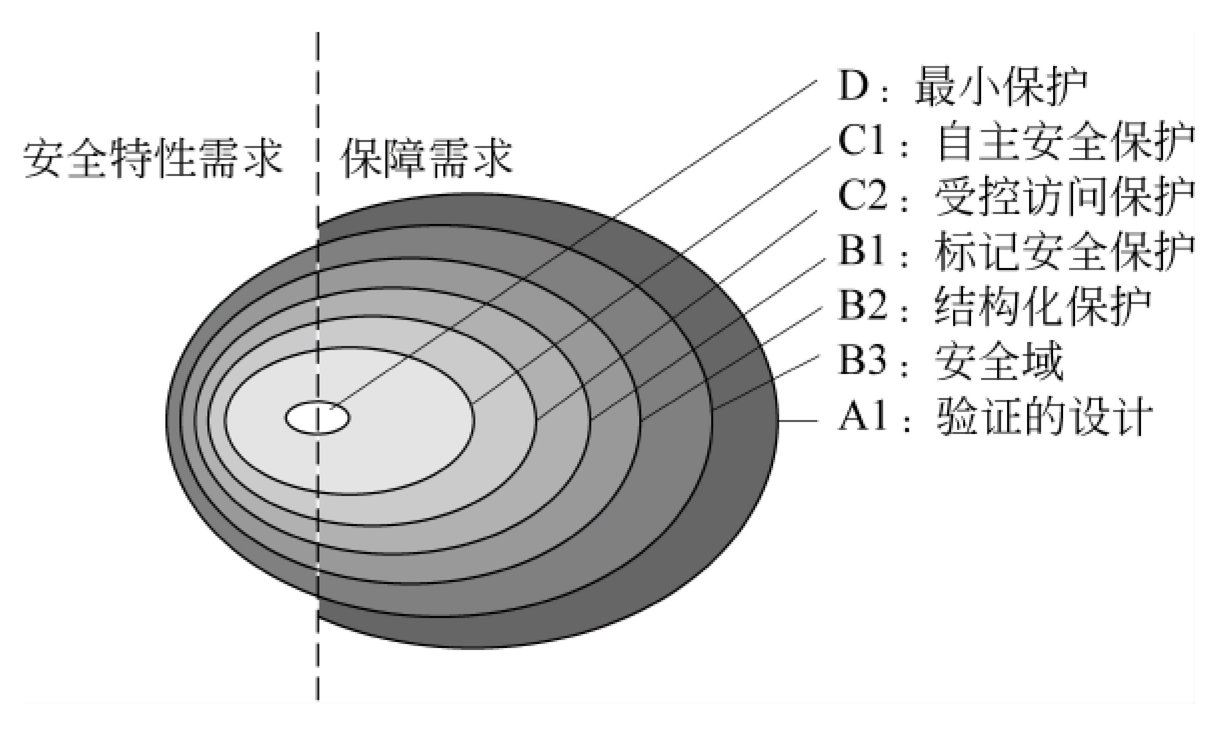


图1-2 TCSEC的构成与等级结构

7个等级的安全特性需求分别如下。

D ：最小保护

C1：自主安全保护

C2：受控访问保护

B1：标记安全保护

B2：结构化保护

B3：安全域

A1：验证的设计

TCSEC 的初衷是主要针对集中式计算的分时多用户操作系统。这套计算机安全的规范与测试评估标准发布之后不久，人们就发现很难将橙皮书应用于网络（分布式）或数据库管理系统（客户服务器结构）。当分布式处理形成规范时，美国国防部又颁布了对橙皮书的附加说明和解释，提高了 TCSEC 标准的实用范围。

1.1.2 ITSEC、CTCPEC 及 FC

1. ITSEC

TCSEC 测评标准应用于非操作系统类比较困难，要求安全产品为了达到某个评估级别，底层操作系统必须完全满足相应的功能要求。新范式的思想就是将通信保密和计算机安全合为一体，通称为信息安全，用于保护信息免受偶然或恶意的非法泄密、转移或破坏，这就是 20 世纪 80 年代末出现的 ITSEC。ITSEC 将安全性要求分为“功能”和“保证”两部分。其中，“功能”指为满足安全需求而采取的一系列技术安全措施，如访问控制、审计、鉴别、数字签名等；“保证”指确保“功能”正确实现及其有效性的安全措施。

ITSEC 根据保证要求定义了 7 个评估级别：E0～E6。

E0：无要求。

E1：有安全目标和 TOE 的描述，满足安全目标的测试。

E2：要求具体设计的描述，测试证据需要加以评估、配置管理、分发控制。

E3：需要进行源代码和结构评估，安全机制的测试证据需要加以评估。

E4：安全策略模型，需要有安全增强功能、架构设计和详细设计。

E5：具体设计和源代码必须相符，并需要使用源代码进行漏洞分析。

E6：TOE 的强制标准、安全策略模型的实施。

功能要求在测定上分 F1～F10 共 10 级。1～5 级对应于 TCSEC 的 D 到 A，6～10 级加上了以下概念。

F6：数据和程序的完整性。

F7：系统可用性。

F8：数据通信完整性。

F9：数据通信保密性。

F10：包括机密性和完整性的网络安全。

表 1-1 所示为 ITSEC 和 TCSEC 的简单对比。

表 1-1 ITSEC 和 TCSEC 的简单对比

级别	ITSEC	TCSEC	级别	ITSEC	TCSEC
1	E0	D	5	F4＋E4	B2
2	F1＋E1	C1	6	F5＋E5	B3
3	F2＋E2	C2	7	F5＋E6	A1
4	F3＋E3	B1			

2. CTCPEC

加拿大可信计算机产品评估准则 CTCPEC vol l.0 于 1989 年公布，专为政府要求而设计。CTCPEC 将安全分为功能性要求和保证性要求两部分。功能性要求为机密性、完整性、可用性和可控性 4 个大类。每种安全要求又分成多级，用于表示安全性上的差别，并按程度不同分为 0～5 级。

3. FC

FC 基于 MSFR 和加拿大的 CTCPEC，其中 MSFR 是 FC 针对 TCSEC 的 C2 级要求提出了适用于商业组织和政府部门的最小安全功能要求。在此标准中首先引入了“保护轮廓(PP)”这一重要概念，每个保护轮廓都包括功能部分、开发保证部分和评测部分，规定了信息产品或系统的技术要求，主要供美国政府使用、民用和商用。

1.1.3 GB 17859—1999

GB 17859—1999 是我国在参考 TCSEC 的基础上制定的国家强制标准，1999 年由国家质量技术监督局发布。GB 17859—1999 规定的计算机系统安全保护能力的 5 个等级分别对应于 TCSEC 中的 C1 级至 B3 级。它在用户自主保护级，即最低级别设立基本安全要求，然后在每一个高安全级别都加入新的需求。

该标准从自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径和可信恢复 10 个方面将计算机信息系统安全保护等级划分为 5 个安全等级。

第 1 级：用户自主保护级，用户自主保护级的计算机信息系统。可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。安全机制包括自主访问控制、身份鉴别、数据完整性。

第 2 级：系统审计保护级。与用户自主保护级相比，系统审计保护级的计算机信息系统中，可信计算基实施了粒度更细的自主访问控制。它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。安全机制包括自主访问控制、身份鉴别、客体重用、审计、自主数据完整性策略。

第 3 级：安全标记保护级，安全标记保护级的计算机信息系统。可信计算基具有系统审计保护级的所有功能。此外，还需要提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述。具有准确地标记输出信息的能力，消除通过测试发现的任何错误。安全机制包括自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、自主和强制数据完整性策略。

第 4 级：结构化保护级，结构化保护级的计算机信息系统。可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第 3 级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素；计算机信息系统可信计算基的接口也必须

明确定义，使其设计与实现能经受更充分的测试和更完整的复审；加强了鉴别机制，支持系统管理员和操作员的职能，提供可信设施管理，增强了配置管理控制。系统具有相当的抗渗透能力。安全机制包括自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、自主和强制数据完整性策略、隐蔽通道分析、可信路径。

第5级：访问验证保护级，访问验证保护级的计算机信息系统。可信计算基满足访问监控器需求，访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的，必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在构造时，排除那些对实施安全策略来说并非必要的代码，在设计和实现时，从系统工程角度将复杂性降低到最小程度；支持安全管理员职能，扩充审计机制，当发生与安全相关的事件时，发出信号；提供系统恢复机制；系统具有很高的抗渗透能力。安全机制包括自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、自主和强制数据完整性策略、隐蔽通道分析、可信路径、可信恢复。

1.1.4 GB/T 18336—2001

《GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则》是中国国家质量技术监督局于2001年发布的推荐标准，该标准的安全功能要求以类、族、组件来表达。类用于对安全要求进行最一般的分组，类中成员覆盖不同的安全目标，但都有一个共同的安全焦点；族包括一套安全要求，满足一个安全目标，但在侧重点和严格性上有差别；组件是族的成员，它描述一个明确的安全要求，是标准定义结构中最小的可选安全要求。标准提供了11个功能类，包括安全审计类、通信类、密码支持类、用户数据保护类、标识与鉴别类、安全管理类、隐秘类、TFS保护类、资源利用类、访问类和可信路径/通道类。以安全审计类为例，它共包括以下6族。

(1) 安全审计自动响应：在检测到可能有安全侵害一类事件时发生的响应。

(2) 安全审计数据产生：对于在TFS控制下发生的安全相关事件，记录其出现的要求。

(3) 安全审计分析：为寻找可能的或真正的安全侵害，用来分析系统活动和审计数据的自动化措施的要求。

(4) 安全审计查阅：可供授权用户查阅审计数据的审计工具的要求。

(5) 安全审计事件选择：在TOE运行期间选择事件来审计的要求。

(6) 安全审计事件存储：TFS能够创建并维护安全的审计踪迹的要求。

1.2 信息技术安全评估通用标准

进入20世纪90年代中期，信息技术安全评估通用标准CC产生，它是加拿大、法国、德国、荷兰、英国和美国6个国家共同努力的成果。CC标准是现阶段最完整的信息技术安全性评估准则。

CC标准将信息技术安全要求分为“功能”和“保证”两大部分。“功能要求”是对产品提供的安全功能或特征的描述，“保证要求”能够让用户相信功能要求能够得到满足，这与

许多国际标准中的区分相类似。CC 定义了安全功能要求的类、族和组件结构划分,提出了常见安全功能要求的 11 个功能类的 135 个功能组件,给 CC 标准的使用者提供直接的参考。用户可以从该结构中选择合适的组件,来定义他们对产品的安全功能要求,编制保护轮廓 PP;开发人员可以选择适当组件定义产品的安全功能,编制安全规范 ST;测评人员同样可以选择适当的组件定义测评内容、编制包。CC 的这种结构形式使得制定标准具有很好的结构性和可操作性。标准起草人仅对部分组件提出了详细具体的规范,对不能详尽规范的组件,只提出了初步的规定,将组件的具体规范留给了标准使用者。CC 也定义了安全保证要求的类、族和部件的结构划分,用于保障 IT 产品或系统满足它的安全目标,安全保证需求使用评估保证级别(EAL)进行区别。

与早期的评估准则相比,CC 的特点体现在其结构的开放性、表达方式的通用性以及结构、表达方式的内在完备性和实用性 4 个方面。

CC 的最基本思想是基于可信的 IT 产品或系统评估,为用户使用产品或系统提供信心保证。

1.2.1 CC 安全测评体系分析

CC 是一个庞大的体系,仅文档就有 1111 页。国内的很多操作系统测评是建立在 CC 标准上的,所以非常有必要对 CC 标准的使用方法以及用 CC 标准进行安全测评的方法、流程和步骤进行分析和总结。

CC 标准的全称是 Common Criteria for Information Technology Security Evaluation,即信息技术安全性评价通用准则。CC 体系一共包括 3 大部分,分别是 Common Criteria for Information Technology Security Evaluation(CC)信息技术安全性评价通用准则、Common Methodology for Information Technology Security Evaluation(CEM)信息技术安全评价通用方法和 Common Criteria Recognition Agreement(CCRA)通用准则识别协议。整个 CC 体系可以通过其官方网站 http://www.commoncriteriaPortal.org 获取。

1. CC 概要

CC 为 IT 产品提供了一系列通用的安全功能需求和安全保证需求,它可以用做安全功能的 IT 产品开发、评价和采购的指导。CC 的体系结构如图 1-3 所示。

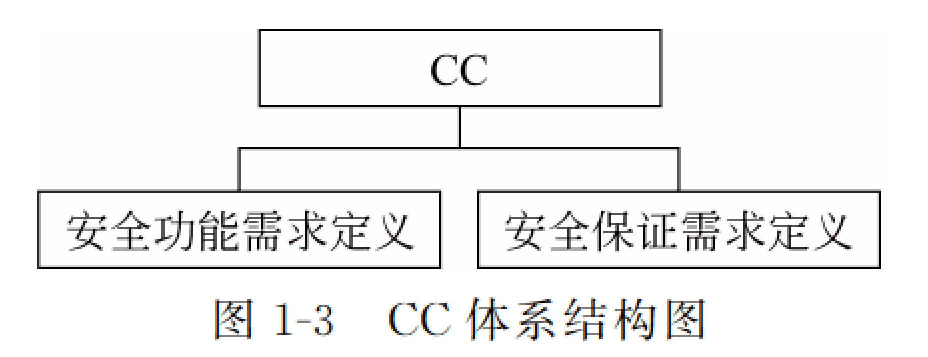


图 1-3　CC 体系结构图

CC 分为 3 个部分,每个部分的内容如下。

第 1 部分:简介和一般模型。该部分是 CC 的总体结构简介,定义了信息技术安全性评估的一般概念和原理,并提出了评估的一般模型。整个评估的过程都要遵循这个一般模型。

第 2 部分:安全功能组件。该部分建立了一系列功能组件,作为 TOE 基本功能需求的标准模板。

第 3 部分:安全保证组件。该部分建立了一系列保证组件,作为 TOE 基本保证需求的标准模板。该部分包括 PP 和 ST 的评价准则等安全保证需求,而且介绍 7 个被称为评

价保证级别的保证包。

2. CC 中的重要概念

CC 标准涉及以下几个关键概念，这几个概念一直贯穿整个 CC 标准。其中的评估对象、保护轮廓、安全目标、组件和包都是 CC 结构的重要组成部分。

（1）评估对象（TOE）。作为安全性评估对象的一系列软件、固件或硬件以及它们的文档，如操作系统、防火墙产品、计算机网络、密码模块等，以及相关的管理员指南、用户指南、设计方案等文档。

（2）保护轮廓（PP）。PP 是一种 TOE 类型的安全需求的独立强制性描述。PP 是用户对安全需求的明确表述。一个 PP 为一类 TOE 基于其应用环境定义了一组安全要求，而不管这些要求具体如何实现，实现问题由“安全目标”来解决。换句话说，PP 与某一个具体的 TOE 无关，它定义的是用户对这类 TOE 的安全需求，规定了一类 TOE 的安全性技术要求以及确保正确有效地实现这些要求的安全保证措施。主要内容如下。

① 需要保护的对象，对该类产品或系统的界定性描述。

② 确定安全环境，如需要保护的资产、已知的威胁、用户的组织、安全策略等。

③ TOE 的安全目的，对安全问题的相应对策，包括技术性和非技术性措施。

④ 信息技术的安全需求，包括功能需求、保证需求和环境安全需求，这些需求通过满足安全目的，进一步提出具体在技术上如何解决安全问题。

⑤ 基本原理，指明安全需求对安全目的、安全目的对安全环境是充分且必要的。

⑥ 附加的补充说明信息。在标准体系中，PP 相当于产品标准，有助于过程规范性标准的开发。国内外现已对应用级防火墙、包过滤防火墙、智能卡、数据库、访问控制、入侵检测、PKI、VPN、网上证券委托等产品或系统开发了相应的 PP。

（3）TOE 安全规范（ST）。ST 的开发是针对具体的 TOE 而言的，它包括该 TOE 的安全目的和能满足安全目的的安全需求，以及为满足安全性技术要求而提供的特定安全性技术要求和保证措施。其中的技术要求和保证措施可以直接引用该 TOE 所属产品或系统类的 PP，可以直接引用 CC 中的安全功能或保证组件，也可以针对具体实际而明确陈述。由于 ST 是对特定 TOE 而开发的，通过安全性评估可以证明该 TOE 所要实现的技术和保证措施，对满足指定安全需求和目的而言是有用和有效的。因此，ST 是开发者、评估者、用户在 TOE 安全性和评估范围之间达成一致的基础，相当于产品或系统的实现方案。由于 ST 与具体的 TOE 实现有关，因此可以满足一个或多个 PP 提出的要求，如某一防火墙的 ST 可能同时满足包过滤防火墙 PP 和应用级防火墙 PP 的要求。

（4）组件（Component）。组件是 CC 的一个关键概念，描述一组特定的安全需求，是可供 PP、ST 或包选取的最小安全需求集合，即将传统的安全需求分成不能再分的块。

（5）包（Package）。组件依据某一特定关系组合在一起，就构成包。构建包的目的是定义那些公认有用的、对满足某一特定安全目的有效的安全要求。包可用于构造更大的包、PP 和 ST 或测评使用。例如，测评人员可以根据将 CC 中某个安全等级指定的组件放在一起，组成一个典型的包——评估保证包。

3. CC各部分的作用

通常,CC只被认为是一个IT安全产品的评价准则。但是,它的作用不仅在于对测评对象的评价,对于IT产品的消费者和开发者都有非常重要的作用。从另一个角度来说,CC关注的不仅是测评,而是整个IT安全产品的生命周期。用户在IT安全产品开发之前,应该通过专业人士的帮助,按照CC安全功能组件,提出对产品的安全需求,即保护轮廓(PP);在产品设计阶段,开发人员应该按照CC安全功能组件,形成对IT安全功能设计的描述(ST);在产品完成之后,认证机构应该根据CC安全保证组件,对PP、ST等进行安全保证的测评和对TOE进行安全功能的测评。

1.2.2 安全功能组件

CC通过“类(Class)—族(Family)—组件(Component)”结构组织安全功能需求。每一个类代表一类安全功能,其中包括类名、类介绍和一个或多个功能族。如图1-4所示,每一个功能类有一个唯一的类名,类介绍表达为了满足安全目的族的共同意图和方法。

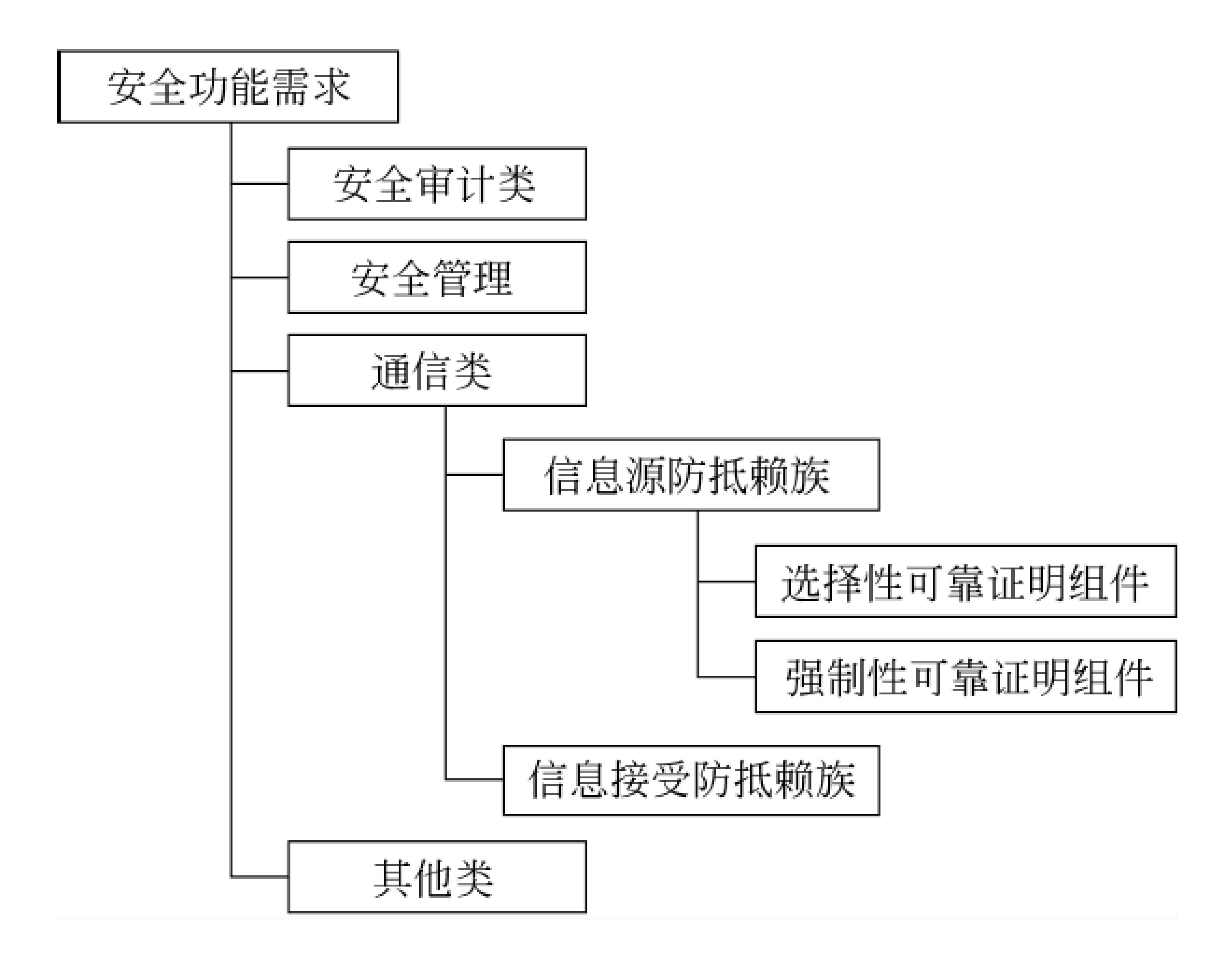


图1-4　安全功能类的组织结构

每个族是更加具体的安全功能分支,内容包括族名、族行为、组件级别、管理、审计和组件。族名也是唯一的标识,是用来提供分类信息的,形式为“XXX-YYY”;族行为是关于功能族的安全目的和功能需求一般性说明的叙述性描述,其中族的安全目的描述了在TOE的帮助下可能被解决的安全问题,族的功能需求总结了所有组件的需求,目的是为了让PP、ST和包的作者用例判定这个族和他们的特定需求是否相关;功能族包括一个或多个组件,每一个都有可能被包含在PP、ST或包中,组件级别通过描述组件的基本原理,为用户提供了选择一个合理的功能组件时所需的信息,一个族中的组件之间有可能有或没有等级关系,如果一个组件提供更多的安全,那么该组件的等级比其他组件高;管理中包含PP/ST作者用做管理行为的信息,涉及FMT类中的组件,提供了关于潜在管理行为的指南,这些管理行为通过操作应用于组件,PP/ST作者可以选择需要的管理组件,或

可以包含其他没有列出的管理需求，来详述管理行为；如果安全审计类被包含在 PP/ST 中，审计才起作用，审计分为最小、一般、详细 3 个级别，描述了每个族中需要审计的内容。

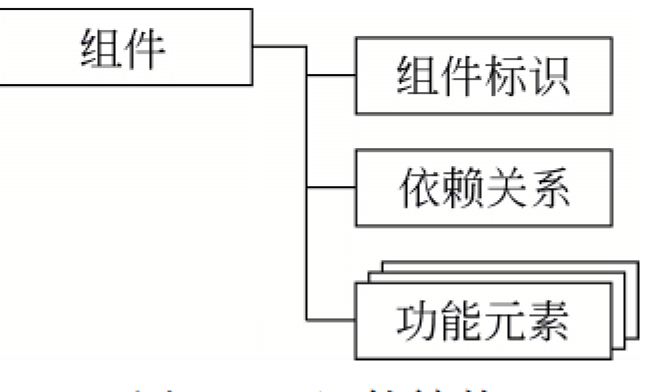


图 1-5 组件结构

组件结构如图 1-5 所示。组件标识描述了鉴别、分类、注册和参照组件时所需的信息，每一个组件都有一个唯一的标识，标识包含一个唯一的标识名、一个标识名缩写和等级列表；功能组件之间可能存在依赖性，组件可能依赖于其他组件的功能性或和其他组件的功能性有交互作用，依赖性提供了组件之间的依赖关系信息，编制 PP、ST 或包时，必须遵守这些依赖关系；组件中包含一个或多个功能元素，每一个元素被独立定义，功能元素是安全功能需求的最小单元，在编制 PP、ST 或包时，不能从组件中只选择一个或多个元素，应该将一个组件中的所有元素包含在 PP、ST 或包中。

安全功能需求共包括 11 个类、66 个族和 135 个组件。这 11 个类分别如下：FAU，安全审计类；FCO，通信类；FCS，密码支持类；FDP，用户数据保护类；FIA，标识与鉴别类；FMT，安全管理类；FPR，用户身份私有类；FPT，TFS 保护类；FRU，资源利用类；FTA，TOE 访问类；FTP，可信路径/通道类。

1.2.3 安全保证组件

安全保证类的组织结构和安全功能需求的组织结构类似。保证类的类名、类介绍、族名、组件标识、组件依赖关系和组件中的元素和功能类的类似，族目的和组件目的分别介绍了保证族、组件的意图；应用提示是包含描述引起使用者注意的应用信息。

安全保证需求共包括 8 个类，38 个族。这 8 个类分别如下：APE，保护轮廓(PP)评估类；ASE，安全目标(ST)评估类；ADV，开发类；AGD，指导文档类；ALC，生命周期类；ATE，测试类；AVA，脆弱性评估类；ACO，组合类。

安全保证中还包含对 7 个 EAL(Evaluation Assurance Levels)级别的定义，内容如下。

EAL1：功能型测试级，证明 TOE 与功能规格的一致。

EAL2：结构性测试级，证明 TOE 与系统层次设计概念一致。

EAL3：工程方法上的测试及验证级，证明 TOE 在设计上采用了积极安全操作系统安全测评研究的工程方法。

EAL4：工程方法上的方法设计、测试和评审级，证明 TOE 采用了基于良好开发过程的安全工程方法。

EAL5：半形式化设计和测试级，证明 TOE 采用了基于严格过程的安全工程方法，并适度应用了专家安全工程技术。

EAL6：半形式化地验证设计和测试级，证明 TOE 将安全工程技术应用到严格的开发环境中，来达到消除大风险，保护高价值资产的目的。

EAL7：形式化地验证设计和测试级，证明 TOE 的所有安全功能经得起全面的形式

化分析。

安全级别和组件之间的关系可以用一张表概括,如表 1-2 所示。每一个安全级别和每个族中的一个或零个组件对应,测评时可以根据需要达到的安全级别选择相应的安全保证组件。例如,如果要对开发类进行安全级别为 EAL7 的测评,需要选择的组件分别是 ADV_ARC1、ADV_FSP6、ADV_IMP2、ADV_INT3、ADV_SPMI 和 ADV_TDS6。

表 1-2　安全级别与组件之间的关系

保证类	保证族	保证组件						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
开发	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6

1.2.4　CC 测评流程

对 CC 测评流程的总结如图 1-6 所示。由图可以看出,CC 测评标准不仅关注信息安全产品的安全功能,而且关注产品的整个生命周期。

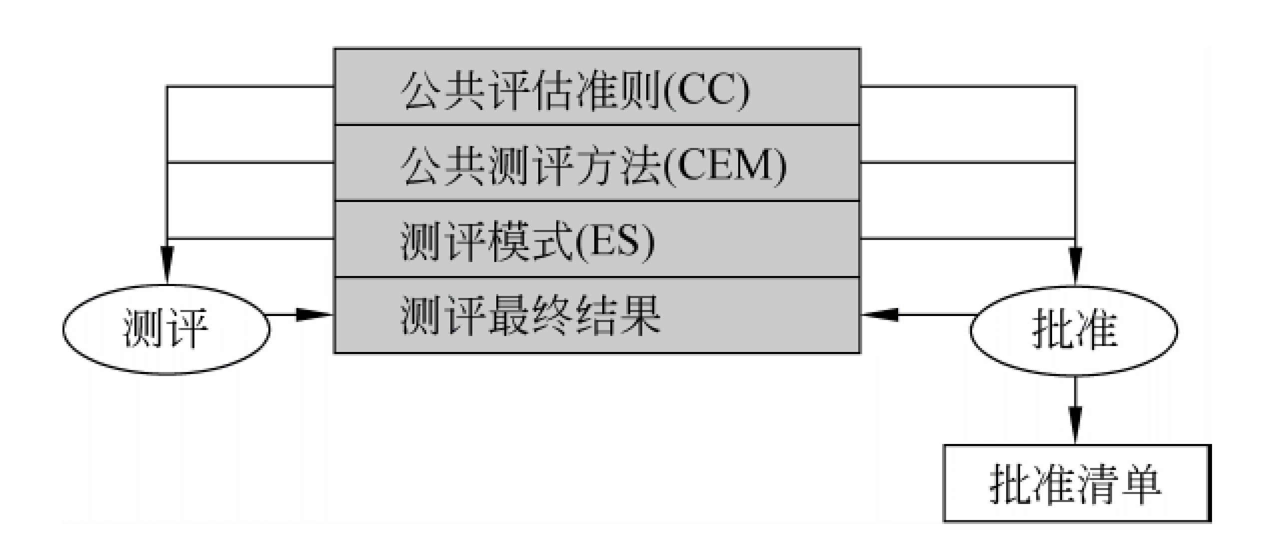


图 1-6　CC 测评流程

1.2.5　CC 评估方法

CEM(公共测评方法)是为了进行 CC 评估而开发的一种国际公认方法。CEM 支撑信息安全评估的国际互认,主要是针对评估者开发的。其他团体,如开发者、发起者、监督者和其他与发布、使用评估结果有关的团体,也都可以从 CEM 中得到一些有用的信息。

评估过程由对开发过程和测试过程所执行的评估行为组成。其中,开发过程和检测过程必须遵循评估方法。也有部分行为,虽然在开发过程和检测过程中,但不在评估过程和 CEM 之中。

CEM 的组织结构和 CC 类似，先介绍了 CEM 的结构和评估模型，之后对 CC 安全保证的每个组件都给出了评估模型中的 4 个任务，即对开发过程和测试过程评估方法的解释，最后介绍了作为证明评估结果依据的基本评估技术，及对脆弱性分析标准的解释和应用实例。

1. 评估方法的组织结构

如同 CC 用类、组件来对安全功能或安全保证进行组织，CEM 以活动、子活动和行为来组织对评估方法的说明。CC 中的类、组件、评估人员行为元素分别和 CEM 中的活动、子活动和行为对应，CC 中的每个保证类在 CEM 中都有一个活动与之对应。每个组件都有子活动相对应，子活动有多个行为，行为详细说明了相关保证组件的评估方法。活动、子活动的分类标识符和 CC 中保证类的类、组件标识符一致。

2. 一般模型

为了消除不正当的压力对评估的影响，CEM 定义了 4 个角色：发起者、开发者、评估者和评估权威机构。发起者负责请求和支持评估，负责建立评估协议(即委任评估)，并且保证评估者提供评估证据。开发者开发 TOE，并且对于提供的评估所需的证据负责(即培训，设计信息)。评估者执行评估任务，评估者代表发起者，从开发者处或直接从发起者处接收评估证据，执行评估子活动并且提供评估结果给评估权威。评估权威机构建立并且维护计划，对评估者的评估进行监督，并且根据评估结果发布检验报告，证明给评估者。

CEM 定义了评估模型，用这个模型来介绍每个族的评估方法。评估模型通常有 4 个任务：输入任务、输出任务、评估子活动及评估人员的评估技术能力范例。输入列出了评估人员评估时需要使用的材料；输出包括观察报告(OR)和评估技术报告(ETR)；评估子活动包含多个行为，即对评估方法的说明。

3. 观察报告和评估报告

输出分为观察报告(OR)和评估技术报告(ETR)。其中 OR 为评估人员提供了一种机制，从评估的角度来澄清和确定问题。如果判定失败，评估人员可以利用 OR 来说明评估结果。

OR 的内容包括以下方面：PP 或 TOE 标识符、得出评估任务/子活动的观察结果、对严重性的评估(例如，指出一个失败的判定、阻止了评估的继续进行、需要在评估完成之前做裁决)、鉴定负责解决这个问题的组织、推荐的解决时间表、没有解决对评估影响的估价。

CEM 给出的评估技术报告(ETR)的结构分为 8 个部分，分别是介绍、TOE 结构描述、评估方法技术和工具、评估结果、结论和建议、评估证据列表、术语表和观察报告。PP 的 ETR 中没有 TOE 结构描述这一项。

4. 评估结果判定定义

CEM 还给出了评估判定的定义。判定分为 4 个层次，即评估行为单元判定、安全保

证组件判定、安全保证类判定、评估结果判定。每个层次的判定都是在其上一个层次基础上做出的，如果上一层有一个以上的失败判定，那这一次的判定也为失败。CEM 认可三种互斥的判定类型是通过、失败和未决定，CEM 对这三种判定给出明确的定义。

1.2.6 通用准则识别协议

通用准则识别协议(CCRA)列出了有 CC 认证授权的参与者(Participant)，例如美国国家安全局、加拿大国家通信安全机构、芬兰国家财政部、希腊内政部等，之后详细叙述了这些机构的权利、职能、管理等方面的要求和规定。

参与者可以授权有资质的认证机构(CBs)，进行 CC 认证的权利，并列出了对这些机构的要求。例如，美国国家信息保证伙伴——通用准则评价和确认计划、加拿大通用准则评价和认证计划等，都是 CBs。

致力于支持该体系的原则，服从和同意现有参与者的国家代表都可以被吸纳为新的 CC 参与者。遗憾的是，中国还没有成为 CC 的参与者。

经过认证授权的 IT 产品，有权利在产品上使用如图 1-7 所示的标志。这个标志表明参与者已经授权 CC 认证。

参与者或授权认证机构则有权利使用如图 1-8 所示的标志来标识它们的身份。



图 1-7　CC 认证标志



图 1-8　CC 授权机构标志

1.3 当前流行操作系统的安全等级

当前主流操作系统的安全性远远不够，如 UNIX 系统、Windows NT 都只能达到 C2 级，安全性均有待提高。在普通操作系统的基础上，各种形式的安全增强操作系统增强了安全性，使得系统的安全性能够满足实际应用的需要。这方面的例子如国内的安胜 3.0 操作系统、作为基于 Linux 核心的安全增强操作系统、达到国标 GB 17859 的第 3 级标准。国外安全操作系统研究的一些新进展，包括 SE Linux 和 EROS 等安全操作系统项目。

1.3.1 Windows 的安全等级

正式获得 C2 级安全等级认证是 Windows NT 4.0，它是基于美国可信计算机系统评测标准 TCSEC 上获得的。事实上，橙皮书仅适用于单机系统，而完全忽视了计算机联网工作时发生的情况。Microsoft 为 Windows NT 获得 C2 安全等级大费周折，只有在计算机未联网、没有网卡，关闭软驱、并在 Compaq 386 上运行时，这个评级才适用。

现在遵循 CC(通用准则,它把系统划分为 EAL 1～7 这 7 级)评估准则,Windows 2000、Windows XP SP2 和 Windows 2003 在 CC 上都是达到 EAL4+级。获得 EAL 4+缺陷修复等级意味着实现了公开大面积销售的商用产品所能达到的最高安全级别。Microsoft 具有识别、修复安全缺陷并分发相应修补程序的规定流程。

1.3.2 Linux 的安全等级

IBM 服务器上执行的红帽操作系统——Red Hat Enterprise Linux 5 的存取控制能力取得了美国政府信息安全认证机构颁发的最高安全等级认证,这意味着那些对信息安全要求较为严格的政府单位可采用红帽的 Linux 操作系统。

此评鉴由 IBM 提出,评估的是在 IBM System x、System p、System z 及 BladeCenter 服务器上执行的 Red Hat Enterprise Linux 5 操作系统。

此次红帽操作系统在三项存取控制部分取得了最高的评估担保等级,包括卷标式安全保护设定文件(Labeled Security Protection Profile,LSPP)、可控制存取保护设定档(Controlled Access Protection Profile,CAPP)及以角色为基础的存取控制保护设定档(Role-Based Access Control Protection Profile,RBAC)。

这并不是 Linux 操作系统首次取得 EAL 4 认证。之前,红帽其他操作系统版本及 Novell 的 Suse Linux 也都曾取得 EAL 4 认证,但这却是 Linux 操作系统首次在存取控制能力上取得该认证。

红帽取得的是国家安全局旗下的国际信息担保组织(National Information Assurance Partnership,NIAP)颁发的第 4 级评估担保等级(Evaluation Assurance Level 4;EAL 4)。NIAP 专门评估商业技术产品的安全性,这也是该组织信息安全等级中最高的一级。

1.3.3 国产操作系统的安全等级

相对来说,中国的安全操作系统研究起步较晚,但也开展了一系列工作。1993 年,国防科技大学开发了基于 TCSEC 标准和 UNIX System V3.2 的安全操作系统 SUNIX。在“COSA 国产系统软件平台”国家“八五”科技攻关项目中,围绕着 UNIX 类国产操作系统 COSIX V2.0 安全子系统的设计与实现工作,中国安全操作系统的研究得到了进一步深入。COSXI V2.0 是一个基于微内核的操作系统,其安全子系统的设计目标是 TCSEC 标准和 B 安全等级,主要安全功能包括安全登录、自主访问控制、强制访问控制、特权管理、审计和可信通路等。1999 年之后,以 Linux 为代表的自由软件在中国的广泛流行,对中国安全操作系统的研究与开发起到了积极的推动作用,相继出现了 LIDS、Soft OS、SeC Linux 等国产安全操作系统。总体来说,目前国内的安全操作系统研究处于上述划分的第二个阶段,以 TCSEC(以及国家标准)为参考而进行。

1. 安胜 OS v4.0

中国科学院软件所设计实现的“结构化保护级”安全操作系统——安胜 OS v4.0 已

通过成果鉴定。该系统是我国首次基于 Linux 源代码研制成功的符合国标《GB 17859—计算机信息系统安全保护等级划分准则》第 4 级要求的高安全等级操作系统，是目前国内安全等级最高的安全信息系统。它是在中科院信息安全技术工程中心承担的中国科学院知识创新工程重要方向项目“结构化保护级安全操作系统设计”支持下完成的。

该项目实现了所要求的全部功能，包括标识与鉴别、自主访问控制、强制访问控制、数据完整性保护、基于角色的最小特权管理、审计、可信通路、客体重用、密码服务、网络安全控制、设备安全控制等，具有新型的体系结构与安全模型。

根据鉴定委员会意见，该项目总体设计合理，技术先进，拥有自主版权的安全内核。突破了国外在高安全等级操作系统上的技术封锁，理论和技术上创新性强，工作量大，技术难度高，达到了国内领先、国际先进水平，首创的隐蔽通道“回溯搜索方法”、三个新型的形式化安全策略模型、安全体系结构等关键技术达到了国际领先水平。

2. 银河麒麟

2006 年 12 月 4 日，国产操作系统——“银河麒麟”操作系统在北京通过国家 863 计划信息领域办公室组织的专家验收。这表明中国拥有自主知识产权、通过认证的安全等级最高的服务器操作系统已研制成功。

国家 863 计划软件重大专项课题——“服务器操作系统内核”由国防科技大学牵头承担。有关科研人员经过 4 年多的艰苦攻关，先后突破一系列核心技术，终于研制成功了这一服务器操作系统。“银河麒麟”操作系统由自主研发的基本内核层和基于 FreeBSD（一种 UNIX 操作系统）改造的系统服务层组成，是一个拥有层次式内核、安全等级达到结构化保护级、能支持多种微处理器和多种计算机体系结构，并与 Linux 目标代码兼容的国产服务器操作系统。

银河麒麟操作系统是针对未来的主流网络服务和高性能计算服务的需求，参照国际主流标准，参考 Darwin、FreeBSD、Linux 和其他商用操作系统，借鉴 UNIX 操作系统和微内核操作系统的设计思想，设计并实现具有自主版权的，可支持多种 CPU 芯片和多种计算机体系结构的，具有高性能、高可用性与高安全性的，并与 Linux 应用和设备驱动二进制兼容的中文服务器操作系统。

中国软件测评中心等有关部门对“银河麒麟”操作系统进行了严格测试和资料、代码审核。结果表明，“银河麒麟”操作系统实现了典型服务器操作系统的全部功能，具有高安全性、高可用性、强实时性、可扩展性和软硬件适配性等特点，系统整体性能与国际主流 UNIX 操作系统相当，部分性能指标以及实时性指标更好。

目前，“银河麒麟”操作系统已在国防领域相关信息系统中得到了成功应用，并形成了一批满足行业用户需求的解决方案，在金融、政府、教育、证券等领域得到应用。图 1-9 是“银河麒麟”操作系统运行界面。

3. Asianux 操作系统

2008 年，红旗软件（中国）、Miracle Linux 公司（日本）和韩软公司（韩国）联合签署了安全 Asianux 操作系统联合开发协议，宣称 Asianux 将成为最先进的安全 Linux 操作系统。

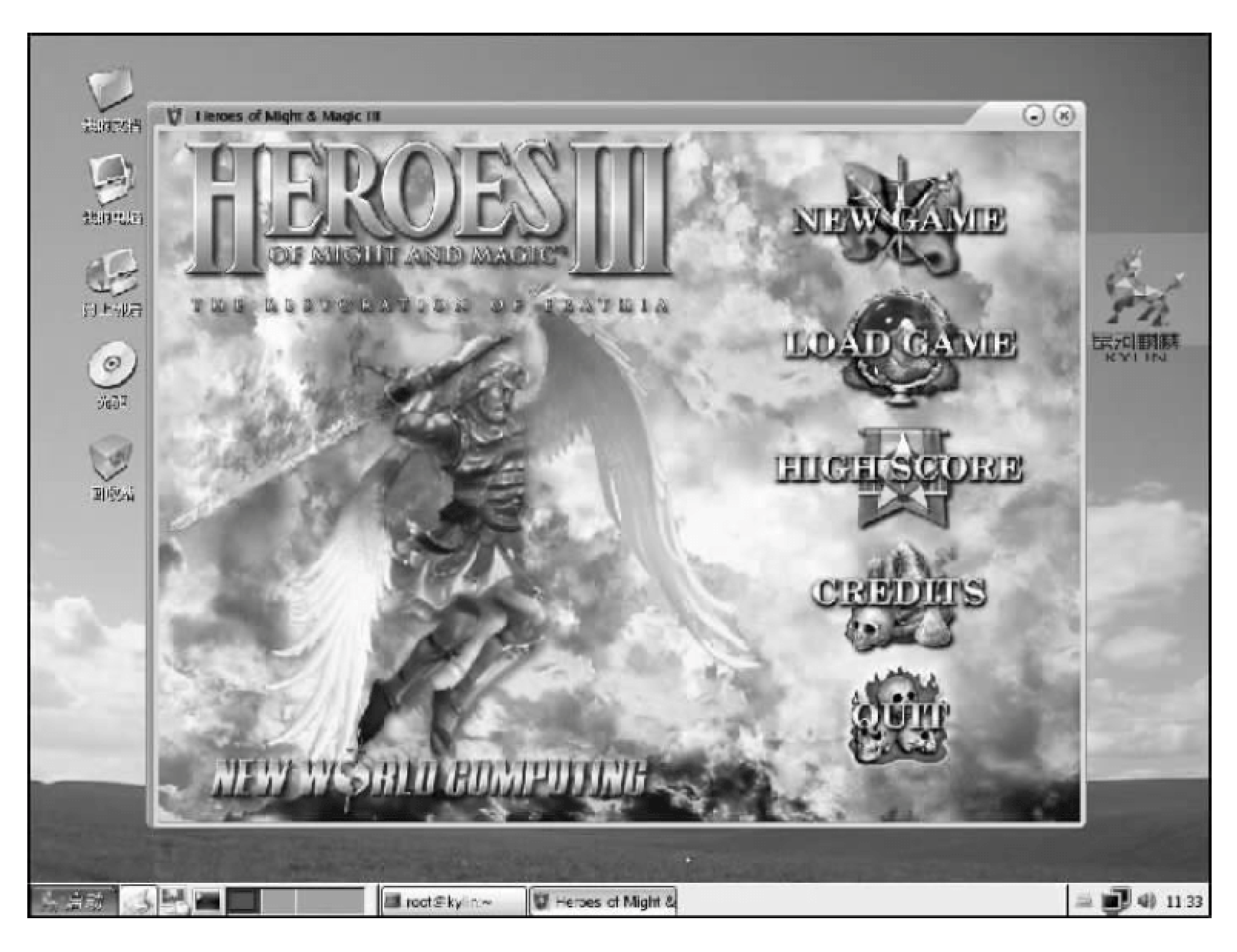


图 1-9 “银河麒麟”操作系统运行界面

习题 1

一、填空题

可信任的计算机系统评价标准 TCSEC 中定义了 A、B、C 和 D 这 4 个安全等级，其中________级别表示计算机系统提供了最强的安全性。

二、选择题

按照 TCSEC 中的定义，Windows 2000 的安全级别为________。

A. A 级　　B. B 级　　C. C1 级　　D. C2 级　　E. D 级

三、判断题

信息技术安全评估公共准则 CC 只是安全准则的集合，并不涉及管理细节和信息安全的具体实现、算法和评估方法等。(　　)

第 2 章　数据链路层安全协议

通信的每一层中都有自己独特的安全问题，网络安全问题应该在多个协议层，针对不同的弱点解决。就安全而言，数据链路层（第二协议层）的通信连接是较为薄弱的环节。本章中，我们将集中讨论与数据链路层相关的安全问题。

数据链路层安全性是指在数据链路各个结点之间能够安全地交换数据。它表现为以下两个方面。

（1）数据机密性。防止在数据交换过程中数据被非法窃听。

（2）数据完整性。防止在数据交换过程中数据被非法篡改。

数据交换过程中的数据机密性和完整性主要是通过密码技术实现的，即通信双方必须采用一致的加密算法对数据机密性和密钥交换算法等问题进行协商，并达成一致协议；在数据交换过程中，通信双方必须按所达成的协议进行数据加密和数据认证处理，以保证数据的机密性和完整性。

数据链路层安全协议增强了数据链路层协议的安全性，即在数据链路层的基础上增加了安全算法协商和数据加密/解密处理的功能和过程。不同的数据链路层协议，其安全协议的功能定义和处理过程是不同的。

2.1　局域网数据链层协议及安全问题

数据链路层主要是为一个网段或一段介质上结点之间的通信提供数据传输服务。数据链路层的所有功能都是针对数据链路而定义的。数据链路层提供了数据链路的差错处理与流量控制功能，将不可靠的数据链路转换成可靠的数据链路，同时完成数据帧的发送与接收，为网络层提供传送数据的功能和过程。

根据网络规模的不同，数据链路层的协议可分为两类：一是本地链路局域网（LAN）中的数据链路层协议，主要通过局域网（LAN）链路，将本地各个结点相互连接起来，实现数据通信。二是针对广域网（WAN）的数据链路层协议，主要通过广域网实现远程结点之间的数据通信。不同物理链路的数据链路层协议是不同的，本地链路的数据链路层协议一般采用 IEEE 802 局域网协议标准，广域网链路的数据链路层协议主要采用点对点协议（PPP）。

2.1.1　IEEE 802 局域网数据链路层协议

IEEE 802 规范定义了网卡如何访问传输介质（如光缆、双绞线、无线等），以及如何在传输介质上传输数据的方法，还定义了传输信息的网络设备之间连接建立、维护和拆除的途径。遵循 IEEE 802 标准的产品包括网卡、桥接器、路由器以及其他一些用来建立局域

网络的组件。

数据链路层包括逻辑链路控制(LLC)子层和介质访问控制(MAC)子层。

逻辑链路控制(LLC),提供终端协议栈的以太网 MAC 和上层之间的接口,其中 LLC 由 IEEE 802.2 标准定义。LLC 子层中规定了无确认无连接、有确认无连接和面向连接 3 种类型的链路服务。无确认无连接服务是一种数据包服务,信息帧在 LLC 实体间交换时,无须在同等层实体间事先建立逻辑链路;有确认无连接服务除对 LLC 帧进行确认外,其他类似于无确认无连接服务;面向连接服务提供访问点之间的虚电路服务,在任何结点帧交换前,一对 LLC 实体之间必须建立逻辑链路,在数据传送过程中,信息帧依次发送,并提供差错恢复和流量控制功能。LLC 子层的主要功能是提供连接服务类型,其中,面向连接的服务能提供可靠的通信。目前,常用 LLC 协议有 CSMA/CD、Token-Bus、Token-Ring 和 FDDI。

MAC 子层的主要功能是控制对传输介质的访问,MAC 子层有如下两个基本职能。

(1) 数据封装,包括传输之前的帧组合和接收中、接收后的帧解析/差错检测。

(2) 介质访问控制,包括帧传输初始化和传输失败恢复。

以太网上的每台计算机都能独立运行,不存在中心控制器。连接到以太网的所有工作站都接入共享信令系统,又称为介质。要发送数据时,工作站首先监听信道,如果信道空闲,即可以帧或数据包格式传输数据。

每帧传输完毕之后,各工作站必须公平争取下一帧的传输机会。对于共享信道的访问,取决于嵌入到每个工作站的以太网接口的介质访问控制机制。该机制建立在载波监听多路访问/冲突检测(CSMA/CD)基础上。

当以太帧发送到共享信道后,所有以太网接口查看它的目标地址。如果帧目标地址与接口地址相匹配,该帧就能被全部读取并发送到那台计算机的网络软件上。如果帧目标地址与它们本身的地址不匹配时,则停止帧读取操作。

了解信号如何通过组成以太网系统的各个介质段,有助于掌握系统拓扑结构。以太网的信号拓扑是一种逻辑拓扑,用来区别介质电缆的实际物理布局。以太网的逻辑拓扑结构提供了一条单一信道(或总线),用于传送以太网信号到所有工作站。

多个以太网段可以连接在一起,构成一个较大的以太网,通过中继器,多段以太网系统可以像无根分支树(non-rooted branching tree)一样扩展。"无根"意味着系统在任意方向上都可以生成连接段,且没有特定的根段。最重要的是,各段的连接不能形成环路。系统的每个段必须具有两个终端,这是因为以太网系统在环路路径上不能正确运行。即使介质段以星状模式物理连接,且许多段都接在中继器上,但是它的逻辑拓扑结构是通过以太网单信道传送信号至所有工作站的。

10/100Mbps 以太网中的基本 IEEE 802.3 MAC 数据格式如图 2-1 所示。

前导码(7字节)	帧起始定界符(1字节)	目的地址(6字节)	源地址(6字节)	长度/类型(2字节)	数据(46字节)	填充(1500字节)	帧校验序列(4字节)

图 2-1 IEEE 802.3 以太网帧结构

(1) 前导码(Preamble)—7 字节。字段中 1 和 0 交互使用,接收站通过该字段知道导

入帧，并且该字段提供了同步化接收物理层帧接收部分和导入比特流的方法。

(2) 帧起始定界符(Start-of-Frame Delimiter)—1 字节。字段中 1 和 0 交互使用，结尾是两个连续的 1，表示下一位是利用目的地址的重复使用字节的重复使用位。

(3) 目的地址(Destination Address)—6 字节。该字段用于识别需要接收帧的站。

(4) 源地址(Source Addresses)—6 字节。该字段用于识别发送帧的站。

(5) 长度/类型(Length/Type)—2 字节。如果是采用可选格式组成帧结构时，该字段既表示包含在帧数据字段中的 MAC 客户机数据大小，也表示帧类型 ID。

(6) 数据(Data)—是一组 $n(46 \leqslant n \leqslant 1500)$ 字节的任意值序列。帧总值最小为 64 字节。

(7) 帧校验序列(Frame Check Sequence)—4 字节。该序列包括 32 位的循环冗余校验(CRC)值，由发送 MAC 方生成，通过接收 MAC 方进行计算，得出以校验被破坏的帧。

2.1.2 局域网数据链路层协议安全问题

通信的每一层中都有自己独特的问题。数据链路层(第二层)的通信连接是较为薄弱的环节，主要的安全问题如下。

1. 共享式以太网中的侦听问题

在共享式以太网中，通信是以广播方式进行的。在理论上，同一广播域内的所有主机都能够访问到在物理媒介上传送的数据包。但在正常情况下，一台网络主机应该只接收与响应两种数据帧：与自己硬件地址相匹配的数据帧和发向所有主机的广播帧。在一个实际的系统中，数据的收发由网卡来完成，每张以太网卡拥有一个全球唯一的以太网地址。它是一个 48 位的二进制数，在以太网卡中内建有一个数据包过滤器，作用是接收以本身网卡的 MAC 地址为通信目的的数据包和广播数据包，丢弃所有其他无关的数据包，以免除 CPU 对无关数据包做无谓的处理，这是以太网卡在一般情况下的工作方式。在这种工作方式下，以太网卡只将接收到的数据包与本机有关的部分向上传递。然而数据包过滤器是可以编程禁用的，禁用后，网卡将把接收到的所有数据包向上传递，上一层的软件因此可以监听以太网中其他计算机之间的通信，这种工作模式为混杂模式(Promiscuous Mode)。多数网卡支持混杂模式，使得采用普通网卡作为网络探针，实现网络的侦听非常容易。这一方面方便了网络管理员，另一方面，普通用户很容易地侦听到网络通信，对用户的数据通信保密是一个很大的威胁。

2. 交换式以太网中的 ARP 广播问题

交换式以太网中监听的实施，除了要借助以太网卡的混杂工作模式外，还利用了 ARP 重定向技术。

ARP(地址解析协议)是 TCP/IP 协议栈的基础协议之一。ARP 提供地址解析服务，用于将 32 位 IP 地址映射到以太网的 48 位硬件地址(MAC 地址)，以便将报文封装成以太帧发送。其间，ARP 的主要功能体现在将上层的 IP 地址与下层的物理地址进行绑定。

ARP 协议虽然是一个高效的数据链路层协议，但是作为一个局域网的协议，它是建立在各主机之间互相信任的基础上的，因此存在一定的安全隐患，内容如下。

(1) 主机地址映射表是基于高速缓存动态更新的，这是 ARP 协议的特色，也是安全问题之一。由于正常的主机间 MAC 地址刷新都是有时限的，如果在下次更新之前成功地修改了被攻击主机上的地址缓存，就可以进行假冒。

(2) ARP 请求以广播方式进行。这个问题是不可避免的，正是由于主机不知道通信对方的 MAC 地址，才需要进行 ARP 广播请求。这样攻击者就可以伪装 ARP 应答，与广播者真正要通信的机器进行竞争。还可以确定子网内的主机什么时候会刷新 MAC 地址缓存，以确定最大时间限度地进行假冒。

(3) 可以随意发送 ARP 应答包。ARP 协议是无状态的，任何主机，即使在没有请求的时候也可以做出应答，只要应答有效，接收到应答包的主机就可以无条件地根据应答包的内容刷新本机高速缓存。

(4) ARP 应答无须认证。ARP 协议是一个局域网协议，设计之初，出于传输效率的考虑，在数据链路层就没有做安全上的防范。在使用 ARP 协议交换 MAC 时无须认证，只要收到来自局域网内的 ARP 应答包，就将其中的 MAC/IP 对刷新到本机的高速缓存中。

根据以上链路层协议的安全漏洞分析，主要的攻击行为如下。

(1) 内容寻址器(CAM)表格淹没：交换机中的 CAM 表格包含了诸如在指定交换机的物理端口所提供的 MAC 地址和相关的 VLAN 参数之类的信息。一个典型的网络侵入者会向该交换机提供大量的无效 MAC 源地址，直到 CAM 表格被填满。这种情况发生时，交换机会向所有的端口发送传输进来的信息，因为这时交换机不能从 CAM 表格中查找出特定的 MAC 地址的端口号。CAM 表格淹没只会导致交换机在本地 VLAN 范围内到处发送信息，所以侵入者只能够看到自己所连接到的本地 VLAN 中的信息。

(2) VLAN 中继：VLAN 中继是一种网络攻击，由一终端系统发出以位于不同 VLAN 上的系统为目标地址的数据包，而该系统不可以采用常规的方法被连接。该信息被附加上不同于该终端系统所属网络 VLAN ID 的标签，或者发出攻击的系统伪装成交换机，并对中继进行处理，以便攻击者能够收发其他 VLAN 之间的通信。

(3) 操纵生成树协议：生成树协议可用于交换网络中，以防止在以太网拓扑结构中产生桥接循环。通过攻击生成树协议，网络攻击者希望将自己的系统伪装成该拓扑结构中的根网桥。要达到此目的，网络攻击者需要向外广播生成树协议配置/拓扑结构，改变网桥协议数据单元(BPDU)，试图迫使生成树进行重新计算。网络攻击者系统发出的 BPDU 声称发出攻击的网桥优先权较低，如果获得成功，该网络攻击者能够获得各种各样的数据帧。

(4) 媒体存取控制地址(MAC)欺骗：在进行 MAC 欺骗攻击的过程中，已知某个其他主机的 MAC 地址会被用来使目标交换机向攻击者转发以该主机为目的地址的数据帧。通过发送带有该主机以太网源地址的单个数据帧的办法，网络攻击者改写了 CAM 表格中的条目，使得交换机将以该主机为目的地址的数据包转发给该网络攻击者。除非该主机向外发送信息，否则它不会收到任何信息。当该主机向外发送信息的时候，CAM 表中对应的条目

会被再次改写,以便它能恢复到原始的端口。

(5) 地址解析协议(ARP)攻击:ARP 协议的作用,是在处于同一个子网中的主机所构成的局域网部分中将 IP 地址映射到 MAC 地址。当有人在未获得授权时就试图更改 MAC 和 IP 地址 ARP 表格中的信息时,就发生了 ARP 攻击。通过这种方式,黑客们可以伪造 MAC 或 IP 地址,以便实施服务拒绝和中间人攻击。

(6) 专用 VLAN:专用 VLAN 通过限制 VLAN 中能够与同 VLAN 中其他端口进行通信端口的方式进行工作。VLAN 中的孤立端口只能和混合端口进行通信。混合端口能够和任何端口进行通信。能够绕过专用 VLAN 安全措施攻击的实现要使用绕过专用 VLAN 访问限制的代理。

(7) DHCP 耗竭:DHCP 耗竭的攻击通过利用伪造的 MAC 地址广播 DHCP 请求的方式来进行。利用诸如 Gobbler 之类的攻击工具,就可以很容易地造成这种情况。如果所发出的请求足够多的话,网络攻击者就可以在一段时间内耗竭 DHCP 所提供的地址空间。这是一种比较简单的资源耗竭的攻击手段,就像 SYN 泛滥一样。然后网络攻击者可以在自己的系统中建立起虚假的 DHCP,对网络上客户发出的新 DHCP 请求作出反应。

根据以上 ARP 协议的安全漏洞,可以进行网络信息包的截获以及 IP 包的转发(重定向)攻击活动,步骤如下。

(1) 把实施攻击主机的网卡设置为混杂模式。

(2) 在实施攻击的主机上保持一个局域网内各个 IP/MAC 包的对应列表,并根据截获的 IP 包或者源 IP 地址进行更新。

(3) 收到一个 IP 分片包之后分析 IP 包头,根据 IP 包头里的 IP 目的地址找到相应的 MAC 地址。

(4) 将本机的 MAC 地址设置成源 MAC 地址,将第(2)步查到的 MAC 地址作为目的 MAC 地址,将收到的 IP 分片包发送出去。

通过以上的重定向,攻击者使网络数据包经过攻击者本身的主机后转发到数据包应该真正到达的目的主机去,因而具有很强的欺骗性。

2.2 局域网数据链路层安全协议

在 IEEE 802 局域网标准中,涉及局域网安全的协议标准主要有 802.10 和 802.1q。

2.2.1 IEEE 802.10

IEEE 802.10 标准是由 IEEE 802.10 标准安全工作组制定的局域网安全标准,其目的是通过加密和认证等安全机制来保证局域网上数据交换的机密性和完整性。

IEEE 802.10 标准原来是为了安全因素而提出的一种帧标签格式。1995 年,Cisco 公司提倡使用 IEEE 802.10 协议,在此之前,IEEE 802.10 曾经在全球范围内作为 VLAN 安全性的统一规范。Cisco 公司试图采用优化后的 IEEE 802.10 帧格式,在网络上传输帧标签

(Frame Tagging)模式中所必需的 VLAN 标签。

为了充分地保护通过共享介质传送的数据流,该协议可以和一个安全管理信息库(Security Management Information Base,SMIB)结合起来使用。它提供了 SAID 和密钥,用于同一安全群组中 LAN 设备之间安全地交换数据。

1. IEEE 802.10 的帧格式

IEEE 802.10 标准定义了一个单独的协议数据单元,通常被称为 Secure Data Exchange(SDE)PDU,也称为 802.10 报头,该标准把 802.10 报头插在了 MAC 地址的帧头和数据区之间。IEEE 802.10 标准定义了一种安全数据交换的协议数据单元,它是在 MAC 帧的帧头和数据域之间插入了一个 802.10 帧头,其格式如图 2-2 所示。

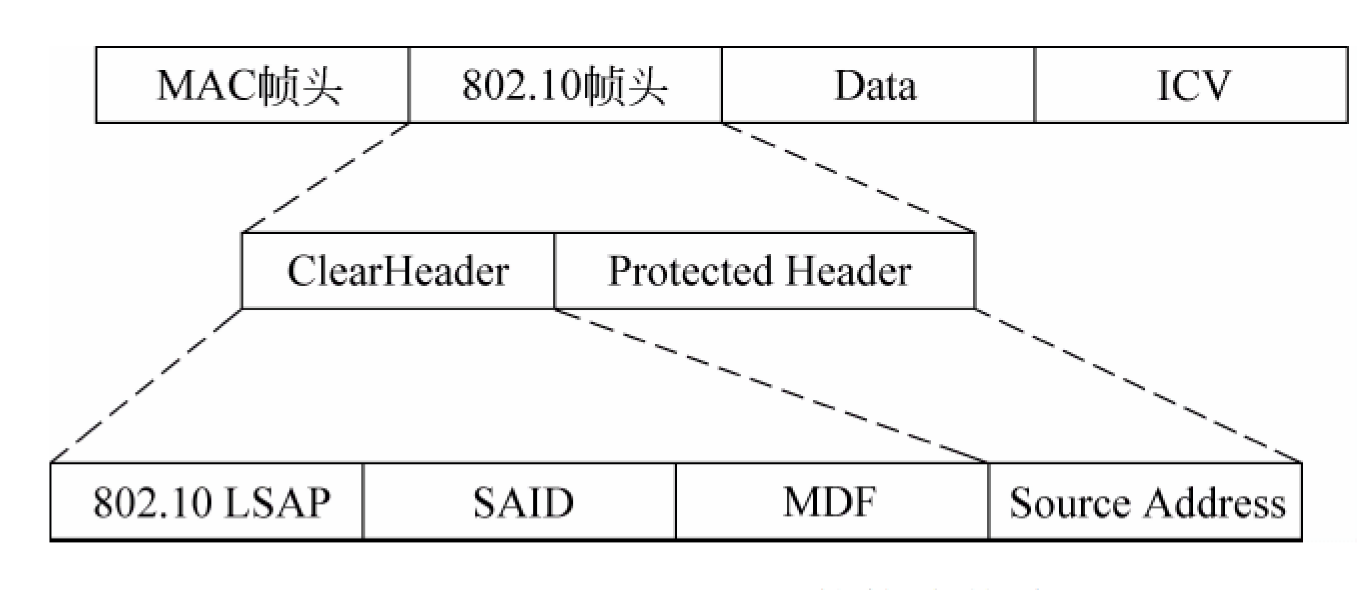


图 2-2 IEEE 802.10 协议头格式

IEEE 802.10 帧头由两部分组成,分别称为 CH(Clear Header)和 PH(Protected Header)。CH 包含一个安全联盟标识符(Security Association Identifier,SAID)字段和一个可选的管理定义字段(Management Defined Field,MDF),以便于 PDU 的处理。PH 包含一个源地址字段,它是从 MAC 头中的源地址字段复制过来的,以支持地址认证功能,防止其他结点冒充源结点。在 LAN 中,每种 MAC 帧都设有一个帧校验序列(FCS)字段,用于对 MAC 帧的正确性和完整性检查,通常 FCS 采用 32 位的循环冗余校验码。因此,每种 MAC 协议本身就具有一定的数据完整性检查能力。IEEE 802.10 完整性检查值(Integrity Check Value,ICV)字段用于数据完整性检查,以防止未经许可对内部数据的修改。为了保证数据机密性,可以对 PH 和 ICV 之间的数据进行加密处理,但由于数据加密将降低网络传输设备(如交换机等)的吞吐能力,引起 LAN 性能的下降,因此 IEEE 802.10 协议中的数据加密功能是可选的,不是强制性规定。

2. IEEE 802.10 的应用模式

IEEE 802.10 协议最初的目的是制定一个互操作的局域网安全标准,但没有得到业界的响应和支持。后来,一些厂商在开发虚拟局域网(VLAN)技术时使用了 IEEE 802.10 头中的 SAID 字段,作为 VLAN 标识符,用于标识数据流所属的 VLAN。这样,IEEE 802.10 协议便在 VLAN 中得到了应用,应用模式拓扑如图 2-3 所示。

VLAN 是指在局域网的物理结构上通过控制流量分配而形成的一种逻辑网络。在一个支持 VLAN 的局域网中,可以按一定的方法和规则构造出多个 VLAN,一个 VLAN 中的流量被限制在本 VLAN 中,不会在其他 VLAN 中流通。这样就使 VLAN 之间在逻

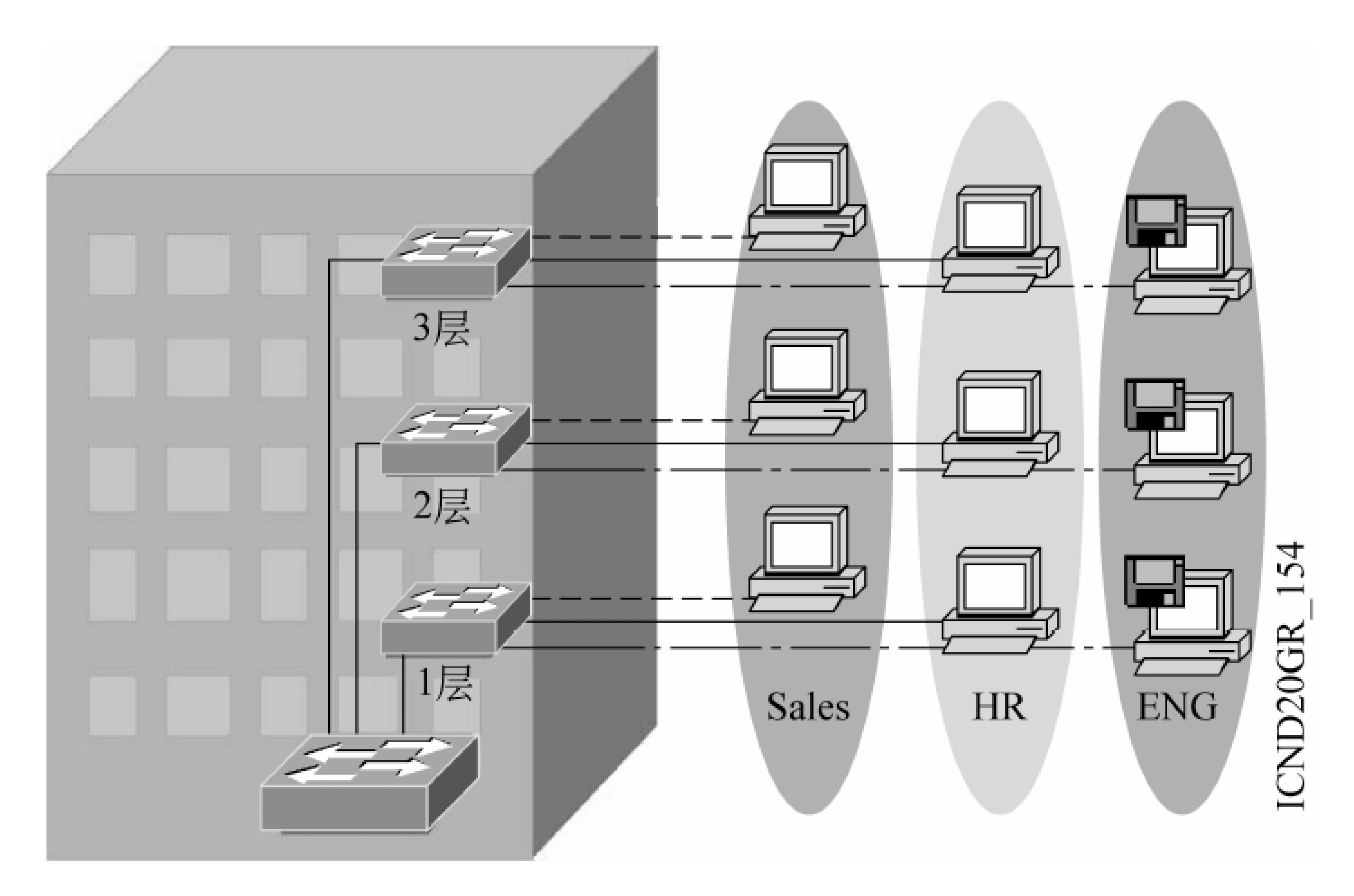


图 2-3　IEEE 802.10 的应用模式

辑上是相互隔离的，VLAN 之间的互通必须通过网桥等设备来实现。因此，通过 VLAN，可以在局域网中保证一定程度的数据交换安全性。通常，VLAN 是在 LAN 交换机支持下实现的，LAN 交换机通过标准化的 VLAN 协议提供 VLAN 定义和管理功能。

由于利用 IEEE 802.10 头中的 SAID 字段作为 VLAN 标识符，导致不定长的数据帧在实现上产生一些问题。另外，各个厂商所定义的 VLAN 标识符格式和长度也不统一，引起不同厂商 VLAN 设备之间的兼容性问题。后来，对 IEEE 802.10 协议进行了修订，进一步完善了 IEEE 802.1q 等新 VLAN 标准，并得到了业界广泛的应用。

2.2.2　IEEE 802.1q

早期 VLAN 在网络之间很难实施，每个 VLAN 都被手动配置在每个交换机上。对 VLAN 的管理，在一个延伸的网络中是非常复杂的任务。为了进一步管理，每个交换机厂商都有不同的方法。为了解决这个问题，开发了 VLAN 干线技术。VLAN 干线通过在帧中加入特定的标签来区分所属的 VLAN，以支持在一个机构中定义多个 VLAN。VLAN 干线是标准化技术，IEEE 802.1q 干线协议就是一个被广泛实施的标准。图 2-4 表示了不同 Cisco 交换机之间的 IEEE 802.1q 干线。

IEEE 802.1q 标准制定于 1996 年 3 月，它规定了 VLAN 组成员之间传输的物理帧需要在帧头部增加 4 个字节的 VLAN 信息，而且还规定诸如帧发送与校验、回路检测、对服务质量参数的支持以及对网管系统的支持等方面的标准。IEEE 802.1q 标准包括 3 个方面：VLAN 的体系结构说明、为在不同设备厂商生产的不同设备之间交流 VLAN 信息而制定的局域网物理帧的改进标准、VLAN 标准的未来发展展望。

IEEE 802.1q 标准提供了对 VLAN 明确的定义及其在交换式网络中的应用。该标准的发布确保了不同厂商产品的互操作能力，并在业界获得了广泛推广，成为 VLAN 发展史上的里程碑。IEEE 802.1q 的出现打破了 VLAN 依赖于单一厂商的僵局，从一个侧面推动了 VLAN 的迅速发展。

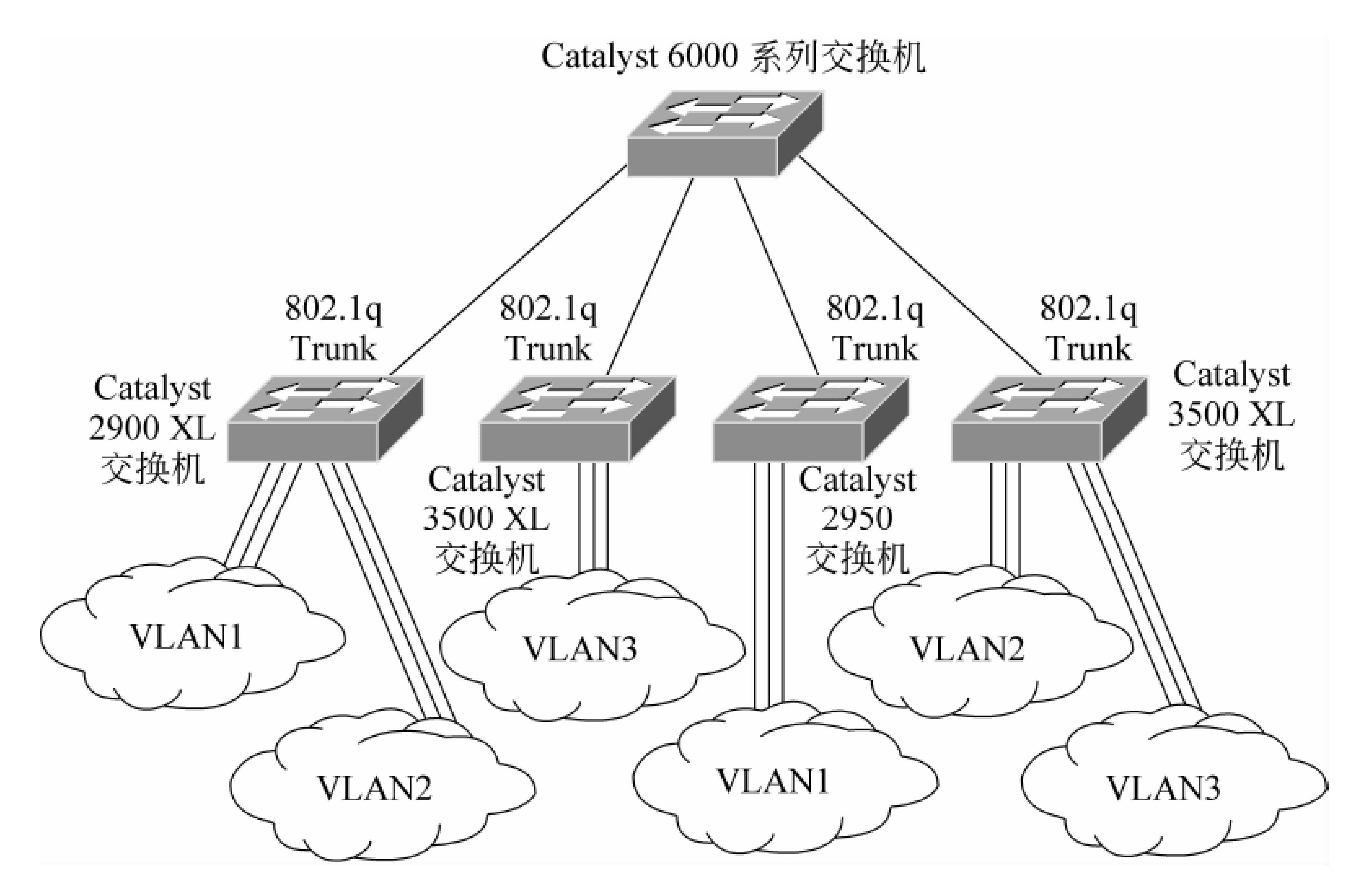


图 2-4　IEEE 802.1q 干线应用

IEEE 802.1q 标准进一步完善了 VLAN 的体系结构，规定统一的 VLAN 标记格式。与 VLAN 相关的协议还有如下内容。

IEEE 802.1p：定义了 VLAN 中数据流优先级标记和动态组播服务，通过定义 8 个优先级，支持不同的数据传输服务级别(Class of Service，CoS)。

IEEE 802.1d：定义了第二层交换机的技术基础和协议标准。

IEEE 802.1p/q 同属一个协议集，使用同一帧格式，它们是在传统的以太网帧格式中插入了一个标记(Tag)字段，占两个字节，如图 2-5 所示。

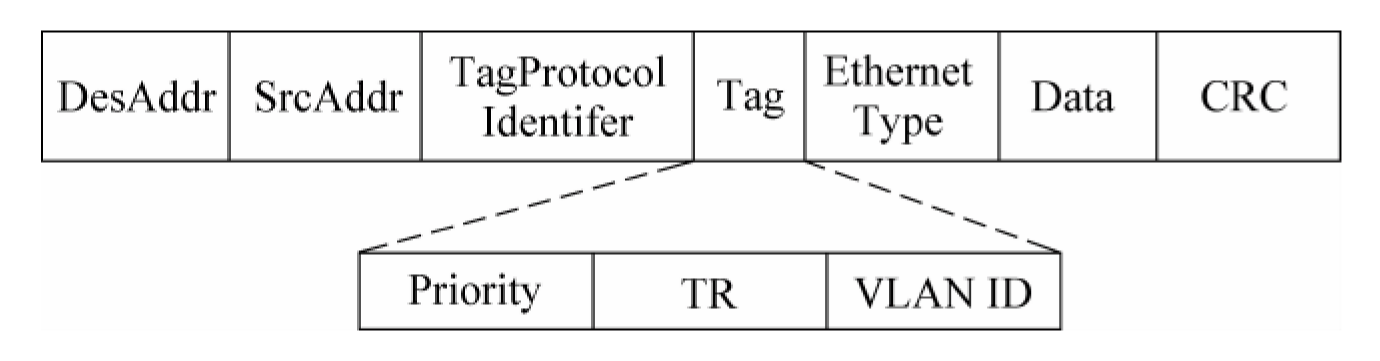


图 2-5　IEEE 802.1q 协议格式

图中，IEEE 802.1p 占 3 位，定义了 8 个优先级；IEEE 802.1q 占 12 位，定义了 VLAN 标识符，用于识别数据流所属的 VLAN。由于 VLAN 标识符共有 12 位，因此一个局域网最多可划分为 4096 个 VLAN。

VLAN 除了提供局域网通信安全性外，还简化了局域网中结点的迁移操作。它既可以在保持结点物理位置不变的情况下，将结点从一个 VLAN 迁移到另一个 VLAN，也可以在保持统一 VLAN 不变的情况下，将结点移动到一个新的物理位置上。所有这些操作通过交换机所配置的 VLAN 管理软件很容易实现。

2.3　广域网数据链路层协议

远程通信是指通过串行接口(RS-232 接口等)和远程链路(如电话线等)实现远程结点之间的数据通信，远程通信协议是建立在远程链路上的数据链路层协议。传统的远程

通信协议是串行线路互联协议(Serial Line Internet Protocol,SLIP),它只是在异步串行链路上提供了对IP协议的最基本支持,而不支持其他非IP数据报传输和同步串行链路通信。在现在的远程通信中,一般采用点对点(Point to Point Protocol,PPP),它提供了在异步或同步串行链路上封装多种协议数据报的方法,能够充分支持IP。

2.3.1 L2F第二层转发协议

第二层转发协议(Level 2 Forwarding protocol,L2F)是一种用来建立跨越公用结构组织(如因特网)的安全隧道,为企业家庭通路连接一个ISP POP的协议。这个隧道建立了一个用户与企业客户网络间的虚拟点对点连接。

第二层转发协议(L2F)允许链路层协议隧道技术。使用这样的隧道,使得分离原始拨号服务器位置,即拨号协议连接终止的位置与提供的网络访问的位置成为可能。

L2F允许在L2F中封装PPP/SLIP包。ISP NAS与家庭网络都需要请求一种常规封装协议,所以可以成功地传输或接收SLIP/PPP包。L2F协议结构如图2-6所示。

1	1	1	1	1	1	1	1	1	1	1	1	1	16	24	32	位
F	K	P	S	0	0	0	0	0	0	0	0	C	Version	Protocol	Sequence	
Multiplex ID														Client ID		
Length														Offset		
Key																

图2-6 L2F协议结构图

(1) Version:用于创建数据包的L2F软件的主修版本。

(2) Protocol:协议字段,规定L2F数据包中传送的协议。

(3) Sequence:当L2F头部的S位设置为1时的当前序列号。

(4) Multiplex ID:数据包Multiplex ID用于识别一个隧道中的特殊链接。

(5) Client ID:Client ID(CLID)支持解除复用隧道中的终点。

(6) Length:整个数据包的长度大小(8位形式),包括头、所有字段以及有效负载。

(7) Offset:该字段规定通过L2F协议头的字节数,协议头是有效负载数据起始位置。如果L2F头部的F位设置为1时,就会有该字段出现。

(8) Key:Key字段出现在将K位设置在L2F协议头的情况。这属于认证过程。

(9) Checksum:数据包的校验和。Checksum字段出现在L2F协议头中的C位设置为1的情况。

2.3.2 PPP协议

PPP(Point-to-Point Protocol,点对点)协议是目前广域网上应用最广泛的协议之一,它的优点在于简单、具备用户验证能力、可以解决IP分配等。家庭拨号上网就是通过

PPP 在用户端和运营商的接入服务器之间建立通信链路。目前，宽带接入正在成为取代拨号上网的趋势，在宽带接入技术日新月异的今天，PPP 也衍生出新的应用。典型的应用是在 ADSL(非对称数据用户环线，Asymmetrical Digital Subscriber Loop)接入方式中，PPP 与其他的协议共同派生出了符合宽带接入要求的新的协议，如 PPPoE(PPP over Ethernet)、PPPoA(PPP over ATM)，如图 2-7 所示。

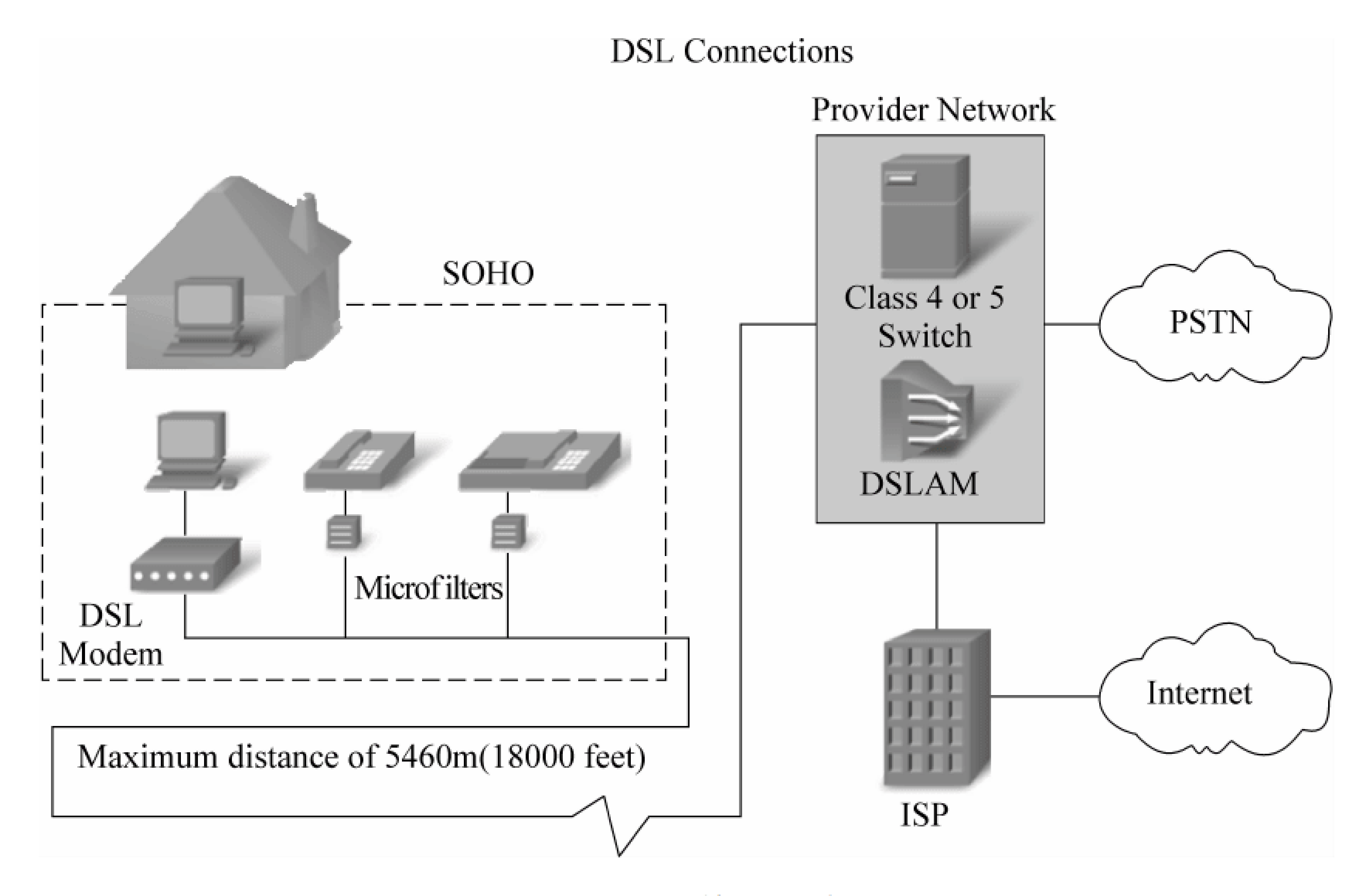


图 2-7　远程接入示意图

利用以太网(Ethernet)资源，在以太网上运行 PPP 来进行用户认证接入的方式称为 PPPoE。PPPoE 既保护了用户方的以太网资源，又完成了 ADSL 的接入要求，是目前 ADSL 接入方式中应用最广泛的技术标准。PPP 协议的简单完整使它得到了广泛应用，在未来的网络技术发展中，它还可以发挥更大的作用。

1. PPP 链路建立过程

PPP 协议中提供了一整套方案来解决链路建立、维护、拆除、上层协议协商、认证等问题。PPP 协议包含这样几个部分：链路控制协议(Link Control Protocol，LCP)；网络控制协议(Network Control Protocol，NCP)；认证协议，最常用的包括口令验证协议(Password Authentication Protocol，PAP)；挑战握手验证协议(Challenge-Handshake Authentication Protocol，CHAP)。

LCP 负责创建、维护或终止一次物理连接。NCP 是一族协议，负责解决物理连接上运行的网络协议类型，以及解决上层网络协议发生的问题。下面介绍 PPP 链路建立的过程，如图 2-8 所示。

一个典型的链路建立过程分为 3 个阶段：创建阶段、认证阶段和网络协商阶段。

阶段 1：创建 PPP 链路。LCP 负责创建链路。在这个阶段，将对基本的通信方式进行选择。链路两端设备通过 LCP 向对方发送配置信息报文(Configure Packets)。一旦一个配置成功信息包(Configure-Ack packet)被发送且被接收，就完成了交换，进入了

LCP 开启状态。应该注意,在链路创建阶段,只是对验证协议进行选择,用户验证将在第2阶段实现。

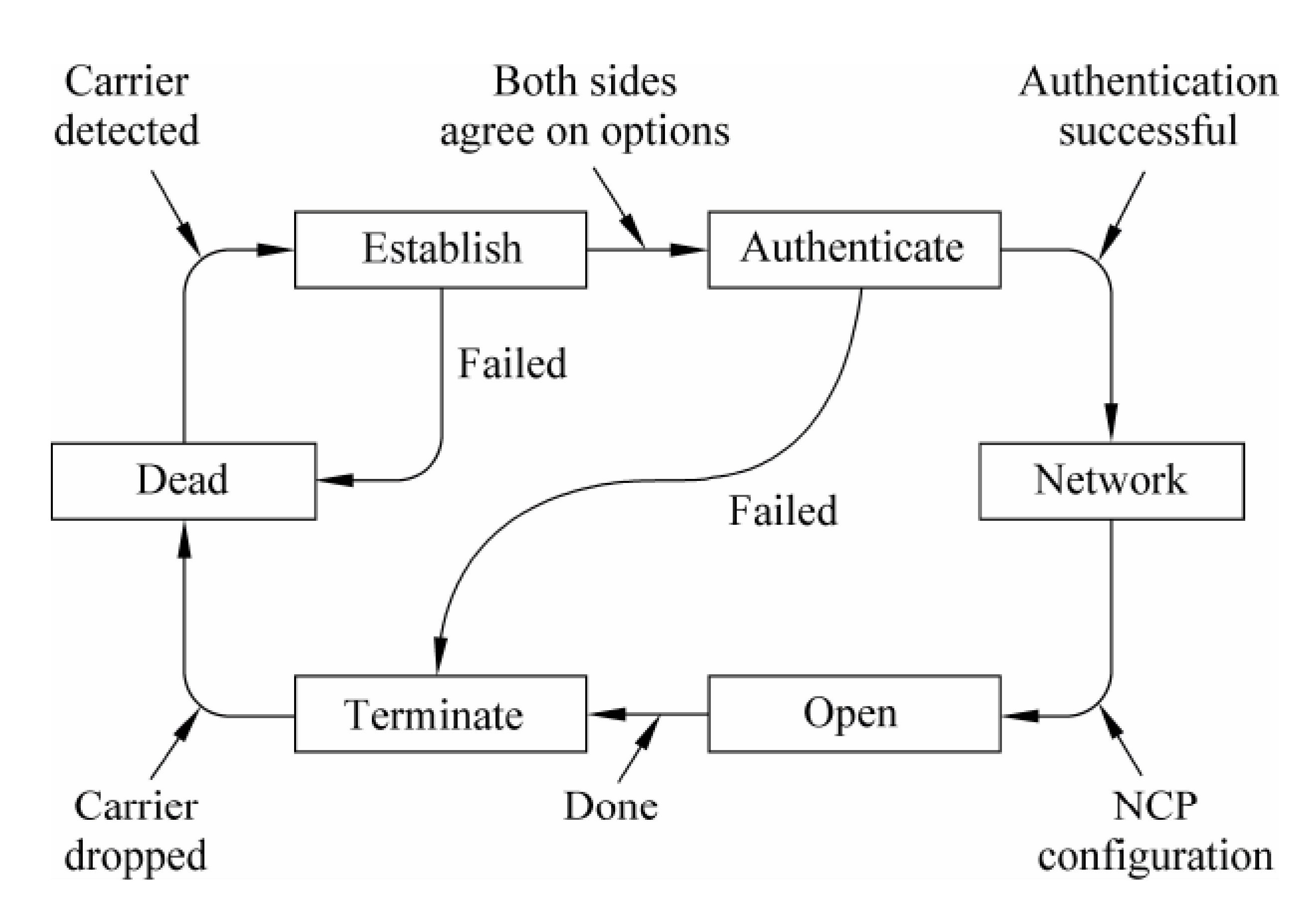


图 2-8 PPP 状态转移图

阶段 2:用户验证。在这个阶段,客户端会将自己的身份发送给远端的接入服务器。该阶段使用一种安全验证方式,避免第三方窃取数据或冒充远程客户接管与客户端的连接。认证完成之前,禁止从认证阶段前进到网络层协议阶段。如果认证失败,认证者应该跃迁到链路终止阶段。在这一阶段里,只有链路控制协议、认证协议和链路质量监视协议的 packets 是被允许的。在该阶段里接收到的其他 packets 必须被丢弃。最常用的认证协议有口令验证协议(PAP)和挑战握手验证协议(CHAP)。

阶段 3:调用网络层协议。认证阶段完成之后,PPP 将调用在链路创建阶段(阶段 1)选定的各种网络控制协议(NCP)。选定的 NCP 解决 PPP 链路之上的高层协议问题。例如,在该阶段 IP 控制协议(IPCP)可以向拨入用户分配动态地址。这样,经过 3 个阶段以后,一条完整的 PPP 链路就建立起来了。

2. PPP 封装

PPP 的帧格式如图 2-9 所示。

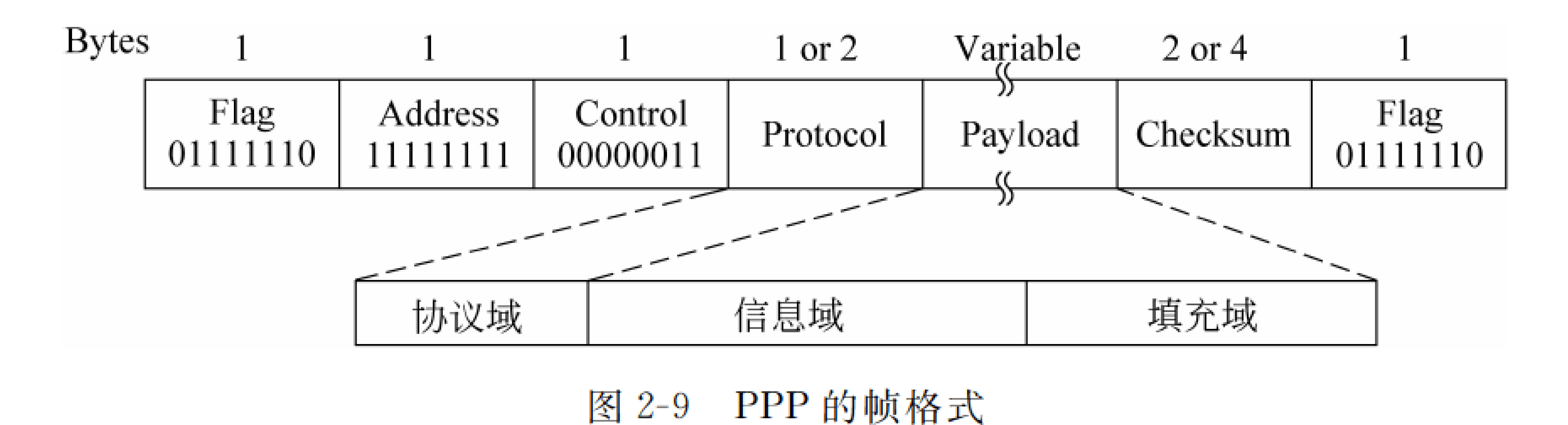


图 2-9 PPP 的帧格式

(1) 协议域:一般为 2 个字节,必要时可压缩为 1 个字节,指出了在信息域中所封装数据报的协议类型,如表 2-1 所示。

(2) 信息域:可以是 0 或多个字节,其中的内容是特定协议类型的数据包,而协议类型由协议域指示。

表 2-1 PPP 帧中协议字段的编码及含义

协议类型编码	所封装的协议类型	协议类型编码	所封装的协议类型
0xc021	连接控制协议 LCP	0x8021	IP 控制协议 IPCP
0xc023	口令认证协议 PAP	0x0021	IP 协议
0xc223	询问-握手协议 CHAP		

(3) 填充域：可以是 0 或多个字节，PPP 可根据需要插入一些附加的填充字节，但填入的字节数不能使信息域和填充域的总长度超过最大接收单元规定的长度(1500 字节)。

PPP 数据包不能直接在物理链路上传输，必须进一步封装成数据帧后才能提交给物理层。因此，PPP 采用 HDLC 结构来封装 PPP 数据包，并对一些特殊控制字符进行了重定义和转义处理。

3. 连接控制协议 LCP

LCP 用于配置、维护和终止 PPP 链路，LCP 定义了 3 种 LCP 数据包，内容如下。

(1) LCP 配置包。其中有配置请求、配置确认、配置否认和配置拒绝 4 种包类型，用于建立和配置 PPP 连接。

(2) LCP 终止包。其中有终止请求和终止确认两种包类型，用于终止 PPP 连接。

(3) LCP 测试包。其中有代码拒绝、协议拒绝、回送请求、回送应答、放弃请求、身份标识和连接剩余时间等包类型，用于管理和测试 PPP 连接。

LCP 数据包是一种协议域为 0xc021 的特定 PPP 数据包，通过代码域定义了上述各种 LCP 数据包，如图 2-10 所示。



图 2-10 LCP 数据包格式

4. 网络控制协议 NCP

NCP 用于在 PPP 连接上建立和配置不同的网络层协议，使得在同一 PPP 连接上可同时传输多种网络层协议的数据包，但通信双方必须配置和使用相同的网络层协议。

PPP 链路连接过程中的 NCP 阶段主要用来建立和配置不同网络层协议，如 IP、IPX 或 AppleTalk。当一个 NCP 处于 Opened 状态时，PPP 将传输相应的网络层协议数据包。当相应的 NCP 不处于 Opened 状态时，任何接收到的网络层协议所支持的数据包都将被丢弃。在这个阶段，链路流量由 LCP、NCP 和网络层协议数据包的任意组合构成。最通用的第三层协商协议为 IP，路由器交换 IP 控制协议(IPCP)信息以协商指定的协议

选项。IPv6 相应的网络控制协议为 IPv6CP。

IPCP 协商两个选项：压缩和 IP 地址指定。但 IPCP 也用于传送网络相关信息，如主要和备份 WINS 名称解析服务以及域名系统(DNS)服务。协议结构如图 2-11 所示。

配置选项格式：

8	16	32	位
Type	Length	Configuration Option	

数据包格式：

8	16	32	variable	位
Code	Identifier	Length	Data	

图 2-11 NCP 帧格式

(1) Code：Code 字段为 8 字节，用于识别数据包类型。

(2) Identifier：Identifier 字段为 8 字节，用于匹配 request 和 reply。

(3) Length：Length 字段为 16 字节，表示数据包长。

(4) Data：Data 字段为 0 或多个字节。Data 字段格式取决于 Code 字段。

5. 认证方式

(1) 口令验证协议(PAP)。PAP 是一种简单的明文验证方式。NAS(Network Access Server，网络接入服务器)要求用户提供用户名和口令，PAP 以明文方式返回用户信息。很明显，这种验证方式的安全性较差，第三方可以很容易地获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接，获取 NAS 提供的所有资源。所以，一旦用户密码被第三方窃取，PAP 无法提供避免受到第三方攻击的保障措施。

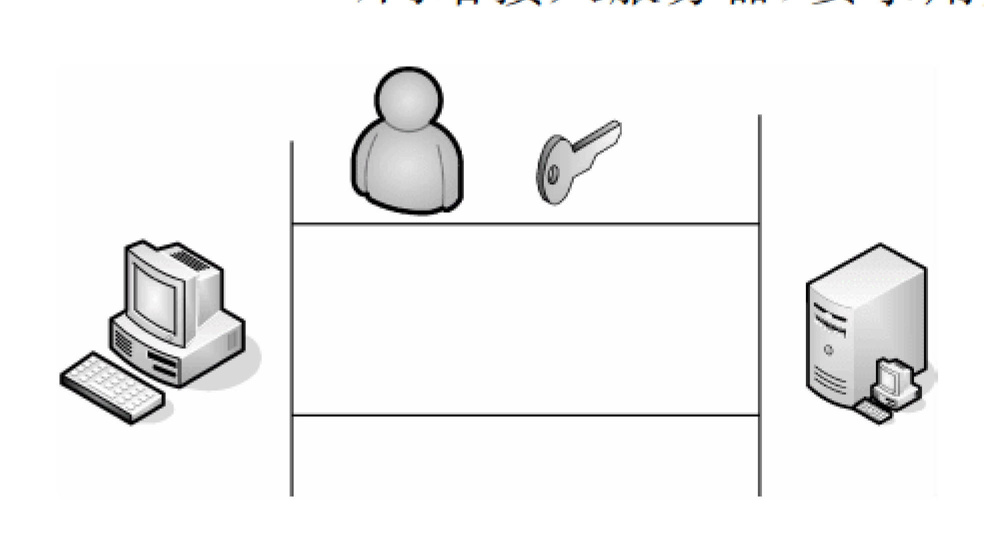


图 2-12 PAP 认证协议流程

PAP 认证协议流程如图 2-12 所示，过程如下。

① 在建立 PPP 连接后，首先由被认证方向认证方发送 PAP 认证请求包，PAP 认证请求中含有标识被认证身份的用户名和口令等认证信息。

② 认证方接收到 PAP 认证请求后，根据认证信息，对被认证方的身份合法性进行认证，然后根据认证结果返回 PAP 认证确认包或 PAP 认证否认包。

③ 如果认证方确认被认证方的身份合法性，则认证过程结束，准备转入传输数据包。否则，重复进行上述的两次握手认证过程，直至确认被认证方的身份合法性，或者重复一定次数后，认证方终止 PPP 连接。

(2) 挑战-握手验证协议(CHAP)。CHAP 是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。NAS 向远程用户发送一个挑战口令(Challenge)，其中包括会话 ID 和一个任意生成的挑战字串(Arbitrary Challenge String)。远程客户必须使用 MD5 单向哈希算法(One-way Hashing algorithm)返回用户名和加密的挑战口令、会话

ID 以及用户口令，其中用户名以非哈希方式发送。

CHAP 对 PAP 进行了改进，不再直接通过链路发送明文口令，而是使用挑战口令，以哈希算法对口令进行加密。因为服务器端存有客户的明文口令，所以服务器可以重复客户端进行的操作，并将结果与用户返回的口令进行对照。CHAP 为每一次验证任意生成一个挑战字串，防止受到再现攻击（Replay Attack）。在整个连接过程中，CHAP 将不定时地向客户端重复发送挑战口令，避免第三方冒充远程客户（Remote Client Impersonation）进行攻击。

CHAP 是三次握手协议，CPAP 认证协议流程如图 2-13 所示，过程如下。

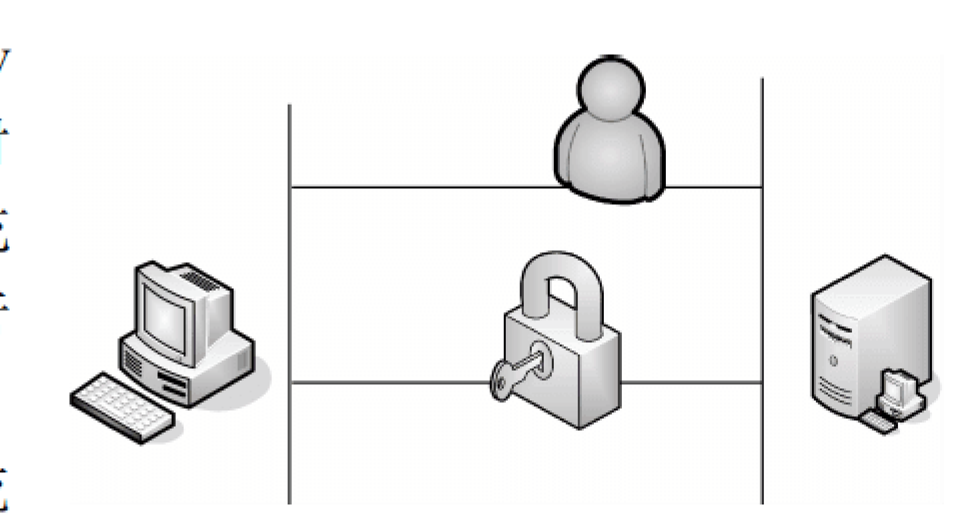


图 2-13　CPAP 认证协议流程

① 在建立 PPP 连接后，首先由认证方向被认证方发送 CHAP 询问包，询问包中含有标识符和询问值等信息。其中，询问值是由提供者随机产生的杂乱字节流，具有全局唯一性和不可预测性，以提高询问值的抗攻击能力。

② 被认证方接收到 CHAP 询问包后，根据 CHAP 询问包中的标识符和询问值，使用单向散列函数计算出响应值，并使用单密钥密码算法加密响应值，然后通过 CHAP 响应包传送给对方，以证明自己的身份。

③ 认证方接收到 CHAP 响应包后，将返回的响应值和期望的响应值进行比较。如果两者相同，则说明对方的身份是合法的，继续维持 PPP 连接；否则，说明对方的身份不是合法的，认证方将终止 PPP 连接。

6. PPP 协议的配置

用户可以在 Cisco 的路由器上配置 PPP 协议。

配置 PPP，在接口配置模式使用 Encapsulation PPP 命令如下：

```
Noko(config)#int s0
Noko(config-if)#encap ppp
Noko(config-if)#^Z
Noko#
```

当然，既然是配置 PPP 连接，就要在两个接口上都进行定义封装格式为 PPP，命令如下：

```
Noco(config)#int s0
Noco(config-if)#encap ppp
Noco(config-if)#^Z
Noco#
```

Configuration PPP Authentication

定义了封装格式后，可以配置验证方式。首先设置路由器的主机名，接下来设置用于

远端连接本地路由器的用户名和密码，格式为在全局模式下使用 username[用户名] password[密码]。命令如下：

```
RouterB(config)#hostname Noco
Noco(config)#username Noko password 4noko
Noco(config)#^Z
Noco#

RouterA(config)#hostname Noko
Noko(config)#username Noco password 4noko
Noko(config)#^Z
Noko#
```

注意：用户名 username 之后跟的是连接本地路由器的那个远程路由器，注意区分大小写。而且两端配置的密码必须一样，因为是明文密码，可以使用 show running-config 来查看密码；可以使用 service password-encryption 来加密密码。

接下来选择验证类型，比如 CHAP 或者 PAP，命令如下：

```
Noco(config)#int s0
Noco(config-if)#ppp authentication chap pap
Noco(config-if)#^Z
Noco#
```

当使用了两种验证方法时，只有第一种方法被使用，第二种作为第一种失败的备份验证方法。

2.3.3 HDLC 协议

1974 年，IBM 公司最先开发出了面向比特的同步协议，称为同步数据链路控制(Synchronous Data Link Control，SDLC)。随后，IBM 公司将此协议提交给 ISO，希望成为国际标准。之后，ISO 对此协议作了修改，并将它重新命名为高级数据链路控制(HDLC)协议。HDLC 是一种数据链路层协议，促进传送到下一层的数据在传输过程中能够准确地被接收(也就是差错释放中没有任何损失并且序列正确)。HDLC 的另一个重要功能是流量控制，换句话说，一旦接收端收到数据，便能立即进行传输。HDLC 具有两种不同的实现方式：高级数据链路控制正常响应模式 HDLC NRM(又称为 SDLC)和 HDLC 链路访问过程平衡(LAPB)，其中第二种使用更为普遍。HDLC 是 x. 25 栈的一部分。

HDLC 是面向比特的同步通信协议，主要为全双工点对点操作提供完整的数据透明度。它支持对等链路，表现在每个链路终端都不具有永久性管理站的功能。另一方面，HDLC NRM 具有一个永久基站以及一个或多个次站。

HDLC LAPB 是一种高效协议，为确保流量控制、差错监测和恢复它要求额外开销最小。如果数据在两个方向上(全双工)相互传输，数据帧本身就会传送所需的信息，从而

确保数据完整性。

帧窗口是用于在接收第一个帧已经正确收到的确认之前发送重复帧。这就意味着在具有长 turn-around 时间滞后的情况下，数据能够继续传送，而不需要停下来等待响应。如卫星通信中常会发生这种情形。

通常，帧分为如下 3 种类型。

(1) 信息帧：在链路上传送数据，并封装 OSI 体系的高层。

(2) 管理帧：用于实现流量控制和差错恢复功能。

(3) 无编号帧：提供链路的初始化和终止操作。

帧格式的结构如图 2-14 所示。

协议结构

1字节	1~2字节	1字节	variable	2字节	1字节
Flag	Address Field	Control Field	Information	FCS	Flag

图 2-14　HDLC 的帧格式

(1) Flag：该字段值恒为 0x7E。

(2) Address Field：定义发送帧的次站地址，或基站发送帧的目的地。该字段包括服务访问点(6 比特)、命令/响应位(表示帧是否与结点发送的信息帧有关或帧是否被结点接收)、地址扩展位(通常设置为 1 字节长)。当设置错误时，表示一个附加字节。

(3) Extended Address：HDLC 为基本格式提供了另一种扩展。通过多方协定，Address Field 可以被扩展为多个字节。

(4) Control Field：识别帧类型。另外，根据帧类型划分，该字段还包括序列号、控制特性和差错跟踪。

(5) FCS：帧校验序列(FCS)字段通过许可传输帧数据的完整性，使高层物理差错控制可以被校验。

2.4　广域网数据链路层安全协议

在广域网两端相应的路由器上，在数据链路层或者网络层增加安全方面配置，提高数据传输的安全。目前，在数据链路层上做安全性保护难度较大，因为涉及的设备种类多、部门多，还有可能需要购买昂贵的安全产品。目前，经常被使用的广域网数据链路层安全协议主要有第二层隧道协议(L2TP)和点对点隧道协议(PPTP)。

2.4.1　第二层隧道协议

第二层隧道协议版本 2(L2TP v2)最初是为远程访问解决方案而设计的，它只支持一种类型的第二层帧：PPP。L2TP v3 保留了版本 2 的许多协议规范，它增强了控制协议，优化了首部封装，可以在分组交换网络上通过隧道传输多种类型的第二层帧。L2TP v3 和它的补充规范描述了适用于使用 L2TP v3 的仿真需求和体系结构。

第二层隧道协议(L2TP)是用来整合多协议拨号服务至现有的因特网服务商提供点。PPP 定义了多协议跨越第二层点对点连接的一个封装机制。特别的,用户通过使用众多技术之一(如拨号 POTS、ISDN、ADSL 等),获得第二层连接到网络访问服务器(NAS),然后在此连接上运行 PPP。在这样的配置中,第二层终端点和 PPP 会话终点处于相同的物理设备中(如 NAS)。

L2TP 扩展了 PPP 模型,允许第二层和 PPP 终点处于不同的包交换网络。通过 L2TP,用户在第二层连接到一个访问集中器(如调制解调器池、ADSL DSLAM 等),然后这个集中器将单独的 PPP 帧以隧道方式发送到 NAS。这样,可以把 PPP 包的实际处理过程与 L2 连接的终点分离开来。

对于这样的分离,一个明显的好处是 L2 连接可以在一个(本地)电路集中器上终止,然后通过共享网络,如帧中继电路或因特网扩展逻辑 PPP 会话,而不用在 NAS 上终止。从用户角度来看,直接在 NAS 上终止 L2 连接与使用 L2TP 没有什么功能上的区别,L2TP 协议也用来解决"多连接联选组分离"问题。多链接 PPP,一般用来集中 ISDN B 通道,需要构成多链接捆绑的所有通道在一个单网络访问服务器(NAS)上组合。因为 L2TP 使得 PPP 会话可以出现在接收会话的物理点之外的位置,它用来使所有的通道出现在单个的 NAS 上,并允许多链接操作,即使是在物理呼叫分散在不同物理位置的 NAS 上的情况下。

L2TP 使用两种信息类型,即控制信息和数据信息。控制信息用于隧道和呼叫的建立、维持和清除,利用 L2TP 中的一个可靠控制通道来确保发送。当发生包丢失时,不转发数据信息;数据信息用于封装隧道所携带的 PPP 帧。L2TP 协议头格式如图 2-15 所示。

														位
											12	16	32	
T	L	X	X	S	X	O	P	X	X	X	X	VER	Length	
Tunnel ID													Session ID	
Ns(opt)													Nr(opt)	
Offset Size(opt)													Offset Pad(opt)	

图 2-15　L2TP 协议头格式

(1) T:T 位表示信息类型。若是数据信息,该值为 0;若是控制信息,该值为 1。

(2) L:当设置该字段时,说明 Length 字段存在,表示接收数据包的总长。对于控制信息,必须设置该值。

(3) X:X 位为将来扩张预留使用。在导出信息中,所有预留位被设置为 0,导入信息中该值忽略。

(4) S:如果设置 S 位,那么 Nr 字段和 Ns 字段都存在。对于控制信息,S 位必须设置。

(5) O:设置该字段时,表示在有效负载信息中存在 Offset Size 字段。对于控制信息,该字段值设为 0。

(6) P:如果 Priority(P)位值为 1,表示该数据信息在其本地排队和传输中将会得到优先处理。

(7) Ver:Ver 位的值总为 002。它表示一个版本 1 L2TP 信息。

(8) Length：信息总长，包括头、信息类型 AVP 以及另外的与特定控制信息类型相关的 AVPs。

(9) Tunnel ID：识别控制信息应用的 Tunnel。如果对等结构还没有接收到分配的 Tunnel ID，那么 Tunnel ID 必须设置为 0。一旦接收到分配的 Tunnel ID，所有更远的数据包必须和 Tunnel ID 一起被发送。

(10) Call ID：识别控制信息应用的 Tunnel 中的用户会话。如果控制信息在 Tunnel 中不应用单用户会话(例如，一个 Stop-Control-Connection-Notification 信息)，Call ID 必须设置为 0。

(11) Nr：期望在下一个控制信息中接收到的序列号。

(12) Ns：数据或控制信息的序列号。

(13) Offset Size & Pad：该字段规定通过 L2F 协议头的字节数，协议头是有效负载数据起始位置。Offset Padding 中的实际数据并没有定义。如果 Offset 字段当前存在，那么 L2TP 协议头在 Offset Padding 的最后八位字节后结束。

2.4.2 点对点隧道协议

点对点隧道协议(PPTP)是一种支持多协议虚拟专用网络的网络技术。通过该协议，远程用户能够通过 Windows 98、Windows XP、Windows Vista、Windows 7 等操作系统以及其他装有点对点协议的系统安全访问公司网络，并能拨号连入本地 ISP，通过 Internet 安全连接到公司网络。

PPTP 可以用于在 IP 网络上建立 PPP 会话隧道。在这种配置下，PPTP 隧道和 PPP 会话运行在两个相同的机器上，呼叫方充当 PNS。PPTP 使用客户机—服务器结构来分离当前网络访问服务器具备的一些功能，并支持虚拟专用网络。PPTP 作为一个呼叫控制和管理协议，允许服务器控制来自 PSTN 或 ISDN 的拨入电路交换呼叫访问并初始化外部电路交换连接。

PPTP 只能通过 PAC 和 PNS 来实施，其他系统没有必要知道 PPTP。拨号网络可与 PAC 相连接，而无须知道 PPTP。标准的 PPP 客户机软件可继续在隧道 PPP 链接上操作。PPTP 使用 GRE 的扩展版本来传输用户 PPP 包。这些增强允许为在 PAC 和 PNS 之间传输用户数据的隧道提供低层拥塞控制和流控制。这种机制允许高效使用隧道可用带宽，并且避免了不必要的重发和缓冲区溢出。PPTP 没有规定特定的算法用于低层控制，但它确实定义了一些通信参数来支持这样的算法工作。PPTP 协议结构如图 2-16 所示。

16	32 bit
Length	PPTP Message Type
Magic Cookie	
Control Message Type	Reserved 0
Protocol Version	Reserved 1
Framing Capability	
Bearing Capability	
Maximum Channels	Firmware Revision
Host Name(64 Octets)	
Vendor String(64 Octets)	

图 2-16 PPTP 协议结构

(1) Length：该 PPTP 信息的八位总长，包括整个 PPTP 头。

(2) PPTP Message Type：信息类型。可能值如下：

① 控制信息；

② 管理信息。

(3) Magic Cookie：Magic Cookie 以连续的 0x1A2B3C4D 进行发送，基本目的是确保接收端与 TCP 数据流间的正确同步运行。

(4) Control Message Type：可能值如下。

① 开始—控制—链接—请求(Start-Control-Connection-Request)。

② 开始—控制—链接—答复(Start-Control-Connection-Reply)。

③ 停止—控制—链接—请求(Stop-Control-Connection-Request)。

④ 停止—控制—链接—答复(Stop-Control-Connection-Reply)。

⑤ 回音—请求(Echo-Request)。

⑥ 回音—答复(Echo-Reply)。

(5) Call Management：可能值如下。

① 导出—呼叫—请求(Outgoing-Call-Request)。

② 导出—呼叫—答复(Outgoing-Call-Reply)。

③ 导入—呼叫—请求(Incoming-Call-Request)。

④ 导入—呼叫—答复(Incoming-Call-Reply)。

⑤ 导入—呼叫—链接(Incoming-Call-Connected)。

⑥ 呼叫—清除—请求(Call-Clear-Request)。

⑦ 呼叫—断开链接—通告(Call-Disconnect-Notify)。

⑧ 广域网—错误—通告(WAN-Error-Notify)。

(6) PPP Session Control：设置—链路—信息(Set-Link-Info)。

(7) Reserved 0 & 1：必须设置为 0。

(8) Protocol Version：PPTP 版本号。

(9) Framing Capabilities：指出帧类型，该信息发送方可以提供如下内容。

① 异步帧支持(Asynchronous Framing Supported)。

② 同步帧支持(Synchronous Framing Supported)。

(10) Bearer Capabilities：指出承载性能，该信息发送方可以提供如下内容。

① 模拟访问支持(Analog Access Supported)。

② 数字访问支持(Digital access supported)。

(11) Maximum Channels：该 PAC 可以支持的个人 PPP 会话总数。

(12) Firmware Revision：若由 PAC 出发，则包括发出 PAC 时的固件修订本编号；若由 PNS 出发，则包括 PNS PPTP 驱动版本。

(13) Host Name：包括发行的 PAC 或 PNS 的 DNS 名称。

(14) Vendor Name：包括特定供应商字串，指当请求是由 PNS 提出时，使用的 PAC 类型或 PNS 软件类型。

2.4.3 L2TP 与 PPTP 的联系与区别

PPTP 和 L2TP 都使用 PPP 协议对数据进行封装，然后添加附加包头，用于数据在互联

网络上的传输。PPTP 协议是点对点隧道协议，其将控制包与数据包分开，控制包采用 TCP 控制，用于严格的状态查询及信令信息；数据包部分先封装在 PPP 协议中，然后封装到 GRE V2 协议中。L2TP 是国际标准隧道协议，它结合了 PPTP 协议以及第二层转发 L2F 协议的优点，能以隧道方式使 PPP 包通过各种网络协议，包括 ATM、SONET 和帧中继。但是 L2TP 没有任何加密措施，更多是和 IPSec 协议结合使用，提供隧道验证。

尽管两个协议非常相似，但是仍存在以下 4 方面的不同。

(1) PPTP 要求互联网络为 IP 网络。L2TP 只要求隧道媒介提供面向数据包的点对点的连接。L2TP 可以在 IP(使用 UDP)、帧中继永久虚拟电路(PVCs)、X. 25 虚拟电路(VCs)或 ATM VCs 网络上使用。

(2) PPTP 只能在两端点间建立单一隧道。L2TP 支持在两端点间使用多隧道，使用 L2TP，用户可以针对不同的服务质量创建不同的隧道。

(3) L2TP 可以提供包头压缩。当压缩包头时，系统开销(overhead)占用 4 个字节，而 PPTP 协议下要占用 6 个字节。

(4) L2TP 可以提供隧道验证，而 PPTP 不支持隧道验证。但当 L2TP 或 PPTP 与 IPSEC 共同使用时，可由 IPSEC 提供隧道验证，无须在第 2 层协议上验证隧道。

2.5 无线局域网数据链路层安全协议

目前，WLAN 业务的需求日益增长，但是相应的安全措施却无法令人满意。最初，人们在研究无线网络的安全问题时，理所当然地把原来应用于有线网络的安全协议植入到无线网络中，但是从 WLAN 安全标准的发展情况看，这种移植的效果还远远未达到要求。从计算机网络诞生的第一天起，无线网络的安全性问题就已成为网络发展的瓶颈，而无线应用的不断增长又使得该问题更彻底地暴露出来。大多数企业都愿意通过有线局域网来传送重要信息，而不用无线局域网，这使得企业虽然确保了信息的安全，却不能利用无线局域网的经济性和灵活性。

目前，IEEE 正致力于消除 WLAN 的安全问题，并在 2004 年年底提出一个新的无线安全标准，来代替现有标准。但是，当前可用的安全协议标准——WEP 并不能使那些重要信息免遭恶意攻击。另外，还有一种过渡期的标准 WPA，它弥补了 WEP 中的大多数缺陷，但也并非完美，IEEE 802.11i 才是下一代无线安全标准。

2.5.1 IEEE 802.11 无线局域网的安全机制

IEEE 802.11 无线局域网运作模式基本分为两种：点对点(Ad Hoc)模式和基本(Infrastructure)模式，如图 2-17 所示。点对点模式指无线网卡和无线网卡之间的直接通信方式，只要 PC 插上无线网卡，即可与另一具有无线网卡的 PC 连接，这是一种便捷的连接方式，最多可连接 256 个移动结点。基本模式指无线网络规模扩充或无线和有线网络并存的通信方式，这也是 IEEE 802.11 最常用的方式。此时，插上无线网卡的移动结点需要通过接入点(Access Point，AP)与另一台移动结点连接。接入点负责频段管理及漫

游管理等工作，一个接入点最多可连接1024个移动结点。当无线网络结点扩增时，网络存取速度会随着范围扩大和结点的增加而变慢，此时添加接入点可以有效控制和管理频宽与频段。

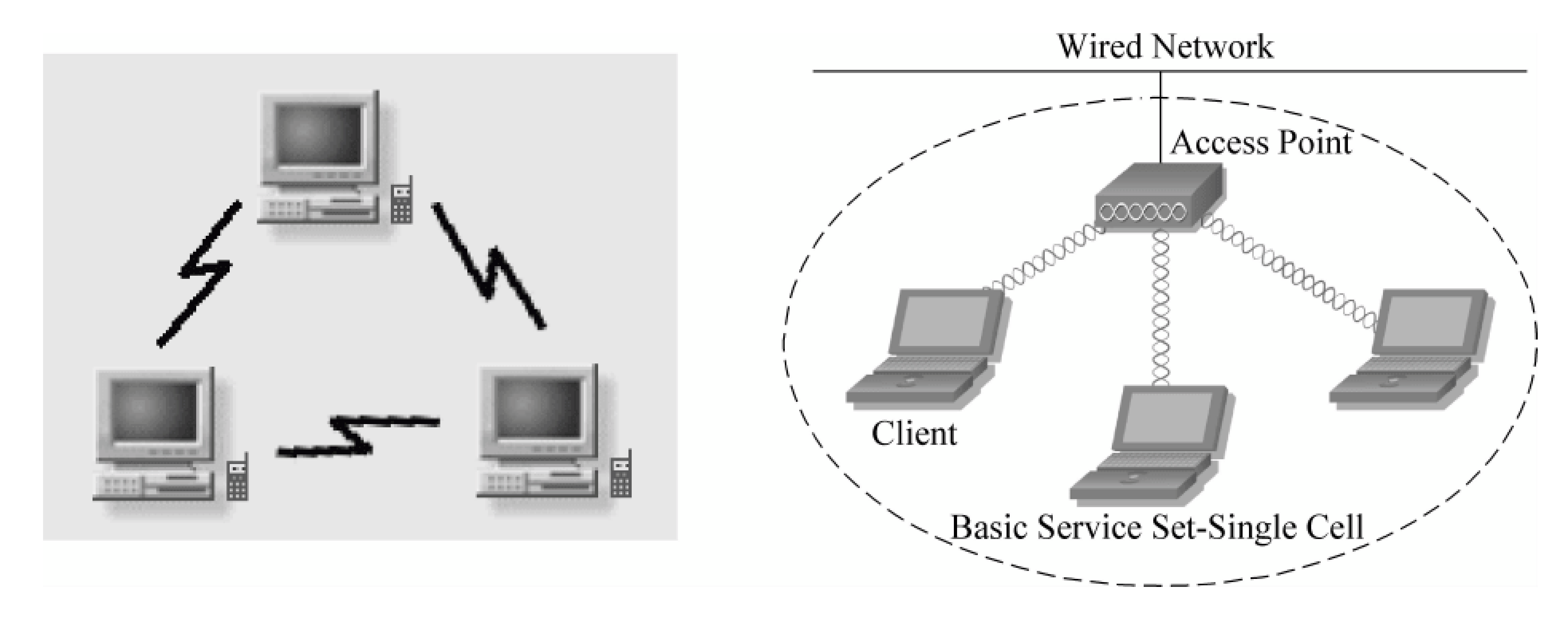


图2-17　无线局域网拓扑结构

与有线网络相比较，无线网络的安全问题具有以下特点。

(1) 信道开放。无法阻止攻击者窃听，恶意修改并转发。

(2) 传输媒质。无线电波在空气中的传播会因多种原因(例如障碍物)发生信号衰减，导致信息的不稳定，甚至会丢失。

(3) 需要常常移动设备(尤其是移动用户)，设备容易丢失或失窃。

(4) 用户不必与网络进行实际连接，使得攻击者伪装为合法用户更容易。由于具有上述特点，利用WLAN进行通信必须具有较高的通信保密能力。

IEEE 802.11无线局域网本身提供了一些基本的安全机制。IEEE 802.11接入点AP可以用一个SSID(Service Set Identifier，服务集标识)或ESSID(Extensible Service Set Identifier)来配置，接入点有关的网卡必须知道SSID，以便在网络中发送和接收数据。但这是一个非常脆弱的安全手段，因为SSID通过明文在大气中传送，甚至被接入点广播，所有的网卡和接入点都知道SSID。

IEEE 802.11的安全性主要包括以有线同等保密(Wired Equivalent Privacy，WEP)算法为基础的身份验证服务和加密技术。WEP是一套安全服务，用来防止IEEE 802.11网络受到未授权用户的访问。启用WEP时，可以指定用于加密的网络密钥，也可以自动提供网络密钥。如果亲自指定密钥，还可以指定密钥长度(64位或128位)、密钥格式(ASCII字符或十六进制数字)和密钥索引(存储特定密钥的位置)。理论上，密钥长度越长，密钥应该越安全。

另外，这一安全机制的一个主要限制是标准没有规定一个分配密钥的管理协议。这就假定了共享密钥是通过独立于IEEE 802.11的秘密渠道提供给移动结点，当这种移动结点的数量庞大时，将是一个很大的挑战。

1. WEP的基本概念

WEP算法主要是防止无线传输信息被窃听，同时也能防止非法用户入侵网络。在一

个运行 WEP 协议的网络上，所有用户都要使用共享密钥，也就是说，用户在终端设备上需要设置密码，并且要和其相连的接入点设置的密码相对应。所有数据包都由共享密钥加密，如果没有这个密钥，任何非法入侵者或企图入侵者都无法解密数据包。但是，WEP 机制自身却存在安全隐患。最大的隐患是许多接入点的配置默认 WEP 项是关闭的，接入点通常采用了默认的出厂配置，这导致了一个巨大的安全漏洞。

即使 WEP 处于开启状态并且设置了新的共享密钥，这一机制也存在极大的隐患。WEP 采用 RC4 加密机制来对数据加密，但问题是 WEP 密钥太易受攻击了，像 AirSnort 和 WEPCrack 这样的应用软件，仅需要抓取 100MB 这么小的流量，在几秒内就能解密受 WEP 保护的网络信息。在大业务量的无线网络中，攻击者可在几分钟内免费接入到 WLAN 中。另外，WEP 使用 CRC 来做数据校验，CRC 很容易被攻击者通过翻转数据包中的比特来破坏可靠性。

WEP 的另一个主要问题是其地址加密，WEP 并不能提供一种方法，以确保合法用户的身份不会被非法入侵者冒充。任何人只要知道 WEP 共享密钥和网络 SSID(服务者身份)，都能接入该网络，当用这些信息来连接网络时，管理者无法判断接纳还是拒绝这一连接。另外，一旦共享密钥被破译或丢失，就必须手动修改所有网络设备的共享密钥，如果密钥丢失而自己又毫不知情，也将是一个安全隐患。

2. WPA 的基本算法

IEEE 802.11i 协议已被 IEEE 批准为正式的 WLAN 安全标准。但 Wi-Fi 联盟要对符合该标准的各种设备进行通用性测试等一系列认证，而很多企业迫不及待地需要一个安全协议。正是由于这种迫切需要，在推出 IEEE 802.11i 之前，Wi-Fi 联盟发布了一个过渡协议 WPA，它可以看做是 IEEE 802.11i 的一个简本。WPA 主要完成了以下工作：解决了 WEP 的主要安全问题，尤其是它在共享密钥上的漏洞；添加了用户级的认证措施；解决了系统的升级问题，传统的 IEEE 802.11b 接入点和无线网卡只需要简单的软、硬件升级，就可以应用 WPA 协议了。

WPA 用新算法解决了 WEP 在加密和数据校验上的缺陷。这些算法就是 TKIP 和 Michael。TKIP 的设计一方面利用了传统接入点中 RC4 算法的硬件加速性能，一方面又避免了 WEP 的缺陷。TKIP 的主要优点就在于它采用了密钥轮转，针对每一个包，它都改变密钥，同时把初始矢量的大小加倍，使网络更安全。因为如果初始矢量很短，并且可被预测，再加上使用静态密钥，无疑给攻击者打开方便之门。Michael 则是完成数据校验的 MIC 算法，一个 MIC 就是一段密文摘要。Michael 算法允许 WPA 系统检查攻击者是否修改了数据包，试图欺骗系统。因为现有很多 IEEE 802.11b 网络接口卡和接入点的处理能力都比较低，因此 Michael 算法专门针对低运算能力进行了设计。也正因为如此，Michael 所能提供的安全保证比同类校验算法要低一些。不过，即使这样，也远远好于 WEP 协议使用的 CRC 算法。接入点在收到包时，会采用 Michael 策略来处理。一旦它发现有两个包都没有通过某个共享密钥的 Michael 算法校验，就会断开这一连接，同时等候一分钟，再创建一个新的连接。然而，这一策略又会让入侵者发起另一种恶意攻击，那就是“拒绝服务”类型的攻击。攻击者会故意发送一些包，让它们无法通过 Michael 算法

校验，这样会引起接入点断掉某一用户的连接。如果不断发起这种攻击，攻击者就能使接入点长期处于下线状态。即使这样，Michael 算法也比没有安全保证要好，虽然攻击者可以切断某个接入点，但 Michael 防止了攻击者进入网络内部，从而造成更大的伤害。

WPA 的另一个缺点是用户和网络间的认证，对于此缺陷使用 IEEE 802.1x 标准进行弥补。

IEEE 802.1x 标准在两个终端间定义了一个扩展的认证协议和一个加密协议 EAPOL (Extensible Authentication Protocol Over LAN)，这个协议可以实现用户到网络的认证。然而 EAP 最初是为有线网络设计的，它首先假定网络和终端设备间的物理连接是安全可靠的，因此对防止窃听几乎无能为力。所以在 WLAN 中，终端和网络间的链路需要加密保护，EAP-TLS(EAP over Transport Level Security)和 PEAP(Protected EAP)等隧道协议提供了这种必需的加密保护。TLS 是安全套接字协议的继承者，后者被广泛应用于 Web 服务中，来保护信息安全。EAP-TLS 是对 TLS 的一个补充，它在用户和服务站点间使用数字证书来实现认证。

虽然在大多数情况下，WEP 将会升级为 WPA，但这两种协议并不能共存。WPA 的硬件如果安装在非 WPA 接入点或者网络接口卡中，将退化为一个 WEP 硬件。WPA 有一个操作模式，允许 WPA 系统和 WEP 系统使用同样的广播密钥，在这种模式下，工作人员应该对 WPA 进行配置，防止同时使用 WPA 和 WEP 进行操作。

2.5.2 IEEE 802.1x 协议的安全机制

1. IEEE 802.1x 协议的体系

IEEE 802.1x 协议起源于 IEEE 802.11，主要目的是为了解决无线局域网用户的接入认证问题。IEEE 802.1x 协议又称为基于端口的访问控制协议，可提供对 IEEE 802.11 无线局域网和对有线以太网络验证的网络访问权限。IEEE 802.1x 协议仅仅关注端口的打开与关闭，对于合法用户接入时，打开端口；对于非法用户接入或没有用户接入时，端口处于关闭状态。

IEEE 802.1x 协议的体系结构主要包括三部分实体：客户端(Supplicant System)、认证系统(Authenticator System)和认证服务器系统(Authentication Server System)，体系结构如图 2-18 所示。

(1) 客户端系统。一般为一个用户终端系统，该终端系统通常要安装一个客户端软件，用户通过启动这个客户端软件发起 IEEE 802.1x 协议的认证过程。

(2) 认证系统。通常为支持 IEEE 802.1x 协议的网络设备。对应于不同用户的端口，该设备有两个逻辑端口，受控(Controlled Port)端口和非受控端口(Uncontrolled Port)。第一个逻辑接入点(非受控端口)，允许验证者和 LAN 上其他计算机之间交换数据，而无须考虑计算机的身份验证状态如何。非受控端口始终处于双向连通状态(开放状态)，主要用来传递 EAPOL 协议帧，保证客户端始终可以发出或接受认证。第二个逻辑接入点(受控端口)，允许经验证的 LAN 用户和验证者之间交换数据。受控端口平时处于关闭状态，只有在

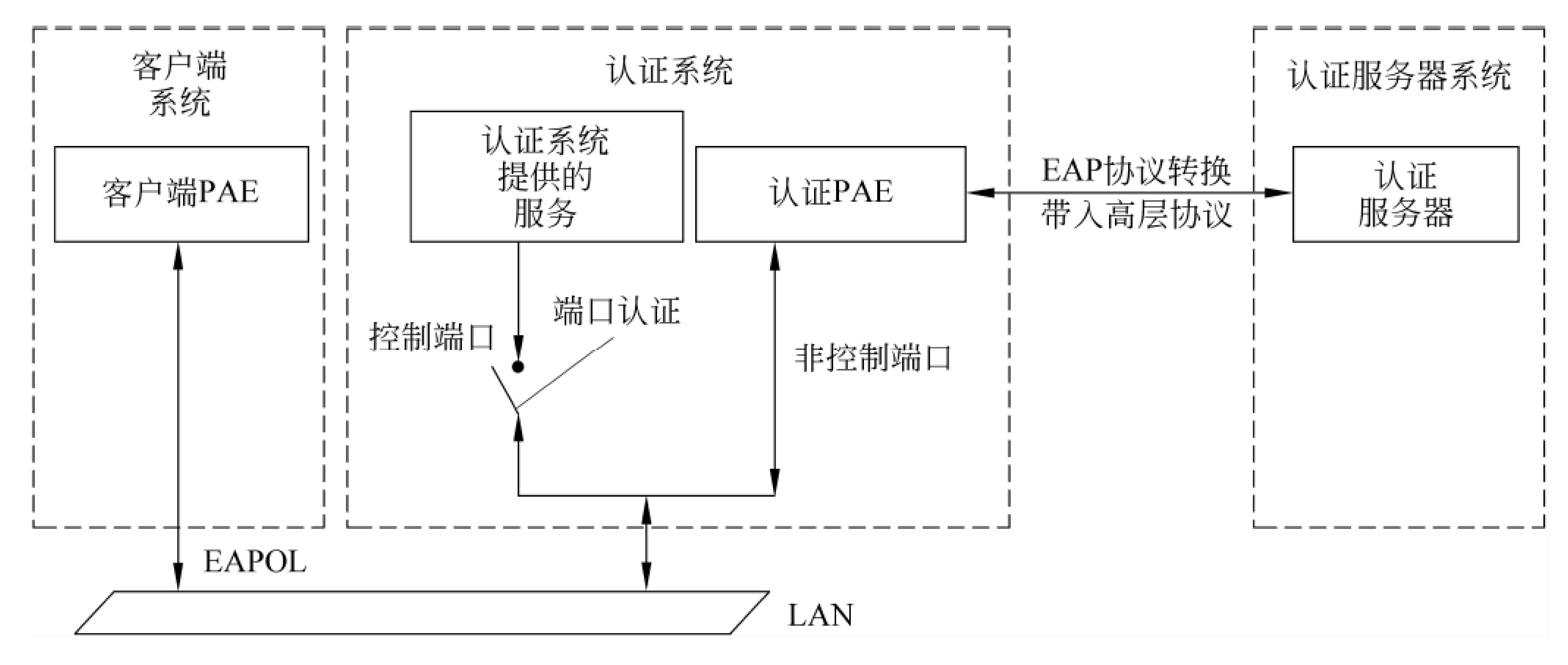


图 2-18　IEEE 802.1x 体系结构图

客户端认证通过时才打开，用于传递数据和提供服务。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用程序。如果用户未通过认证，则受控端口处于未认证（关闭）状态，则用户无法访问认证系统提供的服务。

（3）认证服务器系统。通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户名和口令、用户所属的 VLAN、优先级、用户的访问控制列表等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续数据流就将接受上述参数的监管。

客户系统是 IEEE 802.1x 协议的被认证对象，可以是直接接入认证服务网络的单个用户计算机，也可以是连入认证服务网络设备的一个局域网中的某个用户计算机。该计算机通常需要安装一个客户端软件，用户通过启动这个客户端软件发起请求，进行 IEEE 802.1x 协议的认证，或应答来自认证服务器的要求认证命令。为支持基于端口的接入控制，客户系统必须支持 EAPOL（Extensible Authentication Protocol Over LAN）协议。

在讨论与 IEEE 802.1x 有关的问题时，认证服务代理系统是指“支持 IEEE 802.1x 协议的网络设备的集合”。更确切地讲，它是在所讨论网域中的边界交换设备上支持 IEEE 802.1x 功能的抽象（非边界交换设备不一定需要支持 IEEE 802.1x 的相关功能）。一方面，它属于与客户系统直接相连的交换设备，是直接与客户系统进行认证信息交互的设备，在客户眼中，它就是认证服务系统（虚像），而后台的认证服务器对客户是不可见的，故在本文中将 Authenticator System 译做“认证服务代理”。另一方面，在直接与认证服务器系统相连的边界交换设备中的“认证服务代理”又是客户系统请求认证服务的代理，在认证服务器系统的眼中，它就是“客户系统”（虚像）。换言之，在物理位置上分布的“认证服务代理”作为整体扮演认证服务中介的角色，而在客户系统一侧和认证服务器系统一侧又分别扮演“认证服务代理”和“客户系统代理”的角色。

认证服务器是 IEEE 802.1x 中真正决定是否给客户授权的设备，它借助于认证服务代理的中介作用，与客户系统进行实质性的认证信息交互。为此，它必须存放所有的客户信息和授权规则的控制信息数据库。鉴于 IEEE 802.1x 本身并未定义具体的认证服务应用协议，而只是定义了与认证信息传输相关的协议，因此，要实现认证服务，还必须借助

其他认证服务应用协议。在本文讨论的 IEEE 802.1x 的实现中，利用了 RADIUS（Remote Authentication Dial In User Service）服务机制来实现 IEEE 802.1x 体系结构中的认证应用系统。从这种意义上讲，一个完整的认证服务器实际上由两部分组成：支持 IEEE 802.1x 的认证服务器端口访问实体和 RADIUS 服务器部分，与客户认证相关的控制信息数据库则是建立在 RADIUS 服务器内。

认证服务系统收到消息后，首先由认证服务器端口访问实体处理相关的连接建立请求；再由 RADIUS 服务器查询控制信息数据库，完成用户身份鉴定，并根据授权规则，对通过认证的用户进行授权。

使用 RADIUS 服务器另一个作用如下：RADIUS 服务器还可记录与用户连接有关的其他参数，如允许的最大连接时间和静态 IP 地址等，用于控制用户可控端口的工作时间或计费依据。

有关 IEEE 802.1x 的组成部件的功能，有两点需要再次强调。

（1）从被认证的客户与实现认证的网络运营商之间的关系看，客户通过认证代理间接地与认证服务器打交道，认证服务器对客户是不可见的。

（2）认证代理具有双重性，对客户，它扮演服务器（代理）的角色；对认证服务器，它扮演客户的角色。正如图 2-19 所示，在物理上，是一个整体的认证服务代理端口访问实体（PAE），在概念上，可以看做两个不同的 PAE，一个和客户系统 PAE 通信，一个和认证服务器 PAE 通信。

2. IEEE 802.1x 协议的认证过程

IEEE 802.1x 作为一个认证协议，在实现的过程中有很多状态，图 2-19 说明了其基本认证协议。

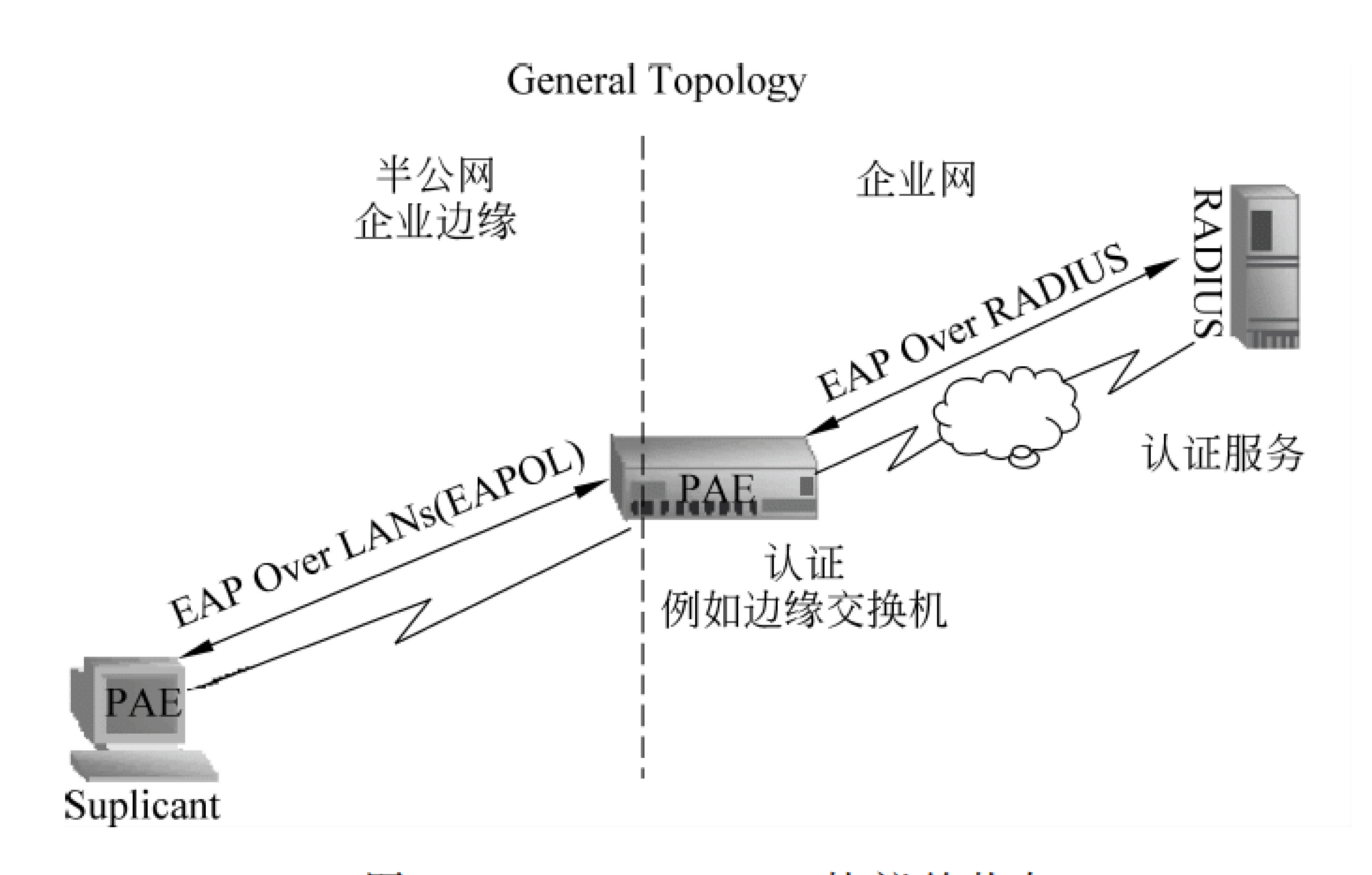


图 2-19　IEEE 802.1x 协议的状态

（1）认证发起。认证可以由用户主动发起，也可以由认证系统发起。当认证系统探测到未经过认证的用户使用网络，就会主动发起认证；用户端则可以通过客户端软件向认证系统发送 EAPOL-Start 报文，发起认证。

① 由认证系统发起的认证。当认证系统检测到有未经认证的用户使用网络时，就会

发起认证。在认证开始之前，端口的状态被强制为未认证状态。

如果客户端的身份标识不可知，则认证系统会发送 EAP-Request/Identity 报文，请求客户端发送身份标识。这样就开始了典型的认证过程。

客户端收到来自认证系统的 EAP-Request 报文后，将发送 EAP-Response 报文，响应认证系统的请求。

认证系统支持定期的重新认证，可以随时对一个端口发起重新认证过程。如果端口状态为已认证状态，则当认证系统发起重新认证时，该端口通过认证，那么状态保持不变；如果未通过认证，则端口的状态改变为未认证状态。

② 由客户端发起认证。如果用户要上网，则可以通过客户端软件主动发起认证。客户端软件会向认证系统发送 EAPOL-Start 报文，主动发起认证。

认证系统在收到客户端发送的 EAPOL-Start 报文后，会发送 EAP-Request/Identity 报文响应用户请求，要求用户发送身份标识，这样就启动了一个认证过程。

(2) 退出已认证状态。有几种方式可以造成认证系统把端口状态从已认证状态改变成未认证状态。

① 客户端未通过认证服务器的认证。

② 由于管理性的控制端口始终处于未认证状态，而不管是否通过认证。

③ 与端口对应的 MAC 地址出现故障(管理性禁止或硬件故障)。

④ 客户端与认证系统之间的连接失败，造成认证超时。

⑤ 重新认证超时。

⑥ 客户端未响应认证系统发起的认证请求。

⑦ 客户端发送 EAPOL-Logoff 报文，主动下线。

退出已认证状态的直接结果就是导致用户下线。如果用户要继续上网，则要再发起一个认证过程。

专门提供一个 EAPOL-Logoff 机制，是出于如下安全的考虑。

当一个用户从一台终端退出后，很可能其他用户不通过发起一个新的登录请求，就可以利用该设备访问网络。提供专门的退出机制，以确保用户与认证系统专有的会话进程被终止，可以防止用户的访问权限被他人盗用。通过发送 EAPOL-Logoff 报文，可以使认证系统将对应的端口状态改变为未认证状态。

(3) 重新认证(根据时间)。为了保证用户和认证系统之间的链路处于激活状态，而不因为用户端设备发生故障造成异常死机，从而影响对用户计费的准确性，认证系统可以定期发起重新认证过程，该过程对于用户是透明的，即用户无须再次输入用户名/密码。

重新认证由认证系统发起，时间从最近一次成功认证后算起。重新认证可以激活或关闭，协议状态参数 reAuthEnabled 控制是否定期进行重新认证。重新认证的时间由参数 reAuthPeriod 控制，默认值为 3600 秒(一个小时)，而且默认重新认证是关闭的。

重新认证的时间设定需要认真规划，认证系统对端口进入的 MAC 地址的检测能力会影响到该时间的设定。如果对 MAC 地址的检测比较可靠，则重新认证时间可以设长一些。

(4) 认证报文丢失重传。对于认证系统和客户端之间通信的 EAP 报文，如果发生丢

失，由认证系统负责进行报文的重传。设定重传时间时，考虑网络的实际环境，通常会认为认证系统和客户端之间报文丢失的几率比较低，以及传送延迟低，因此一般通过一个超时计数器来设定，默认重传时间为30秒。

对于有些报文的丢失，重传比较特殊，如EAPOL-Star报文的丢失，由客户端负责重传；而对于EAP-Failure和EAP-Success报文，由于客户端无法识别，认证系统不会重传。如果EAP-Failure或EAP-Success报文发生丢失，则客户端会在auth-While计数器超时后自动转变为CONNECTING状态。

由于对用户身份合法性的认证最终由认证服务器执行，认证系统和认证服务器之间的报文丢失重传也很重要。

另外需要注意，对于用户的认证，在执行IEEE 802.1x认证时，只有认证通过后，才有DHCP发起(如果配置为DHCP的自动获取)和IP分配过程。由于客户终端配置了DHCP自动获取，则可能在未启动IEEE 802.1x客户端之前就发起了DHCP的请求，而此时认证系统处于禁止通行状态，这样认证系统会丢掉初始化的DHCP帧，同时会触发认证系统，发起对用户的认证。

由于DHCP请求超时过程为64s，所以如果IEEE 802.1x认证过程能在这64s内完成，则DHCP请求不会超时，能顺利完成地址请求；如果终端软件支持认证后再执行一次DHCP，就不用考虑64s的超时限制。

3. 两种类型的报文格式

(1) EAPOL报文格式。IEEE 802.1x协议中定义了一种封装技术，称为EAPOL(EAP over LANs)，主要在客户端和认证系统之间传送EAP协议报文，可以允许EAP协议报文在LAN上传送。EAPOL的帧结构如图2-20所示。

	Octer Number
PAE Ethernet Type(7.5.1)	1~2
Protocol Version(7.5.3)	3
Packet Type(7.5.4)	4
Packet Body Length(7.5.5)	5~6
Packet Body(7.5.6)	7~N

图2-20　EAPOL的帧结构

PAE Ethernet Type：两个字节，表示协议类型，IEEE 802.1x分配的协议类型为888E。

Protocol Version：1个字节，表示EAPOL帧的发送方所支持的协议版本号。本规范使用值为00000001。

Packet Type：1个字节，表示传送的帧类型。有如下5种帧类型。

① EAP-Packet：值为00000000，表示为EAP帧。

② EAPOL-Start：值为00000001，表示为EAPOL-Start帧。

③ EAPOL-Logoff：值为00000010，表示为EAPOL-Logoff请求帧。

④ EAPOL-Key：值为00000011，表示为EAPOL-Key帧。

⑤ EAPOL-Encapsulated-ASF-Alert：值为00000100。

Packet Body Length：2个字节，表示Packet Body的长度。

Packet Body：如果Packet Type为EAP-Packet、EAPOL-Key或EAPOL-Encapsulated-ASF-Alert的值，则Packet Body对应相应的值；对于其他帧类型，则该值为空。

在EAPOL帧传送过程中，不带IEEE 802.1q的VLAN标记，但是可以带IEEE 802.1p的优先级标记。所有的PAE都能够接收带或不带优先级标记的EAPOL帧。

EAPOL帧发送时，当客户端和认证系统互相之间不知道发送的目标时，其目标MAC地址为IEEE 802.1x协议中分配的组播地址01-80-c2-00-00-03。

(2) EAP报文格式。EAP的帧结构如图2-21所示。

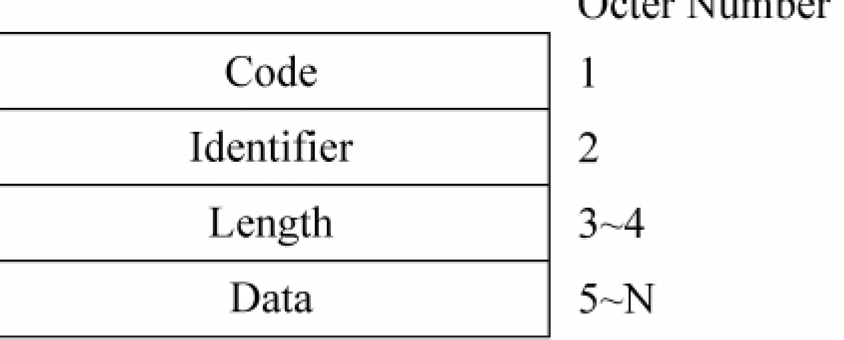


图2-21 EAP的帧结构

Code：1个字节，表示EAP帧类型。EAP代码分配如下：

```
1  Request
2  Response
3  Success
4  Failure
```

Identifier：1个字节，该值用于匹配requests的请求。Identifier区域和系统端口一起，单独标识一个认证过程。

Length：2个字节，该值表示EAP帧的总长度。

Data：0或多个字节，表示数据。

4. 基本的认证过程

IEEE 802.1x协议又称为基于端口的访问控制协议，可提供对IEEE 802.11无线局域网和对有线以太网络验证的网络访问权限。

(1) 以太网认证过程。对以太网验证的状态如图2-22所示，认证的步骤如下。

① 用户开机后，通过IEEE 802.1x客户端软件发起请求，查询网络上能处理EAPOL(EAP Over LAN)数据包的设备。

② 如果某台验证设备能处理EAPOL数据包，就会向客户端发送响应包，并要求用户提供合法的身份标识，如用户名/密码。

③ 客户端收到验证设备的响应后，会提供身份标识给验证设备。

④ 由于此时客户端还未经过验证，因此认证流只能从验证设备的未受控逻辑端口经过。验证设备通过EAP协议，将认证流转发到AAA服务器，进行认证。如果认证通过，则受控逻辑端口打开。

⑤ 客户端软件发起DHCP请求，经认证，设备转发到DHCP Server。

⑥ DHCP Server为用户分配IP地址。认证设备记录用户的相关信息，如MAC、IP地址等信息，并建立动态的ACL访问列表，以限制用户的权限。

⑦ 当认证设备检测到用户的上网流量，就会向认证服务器发送计费信息，开始对用

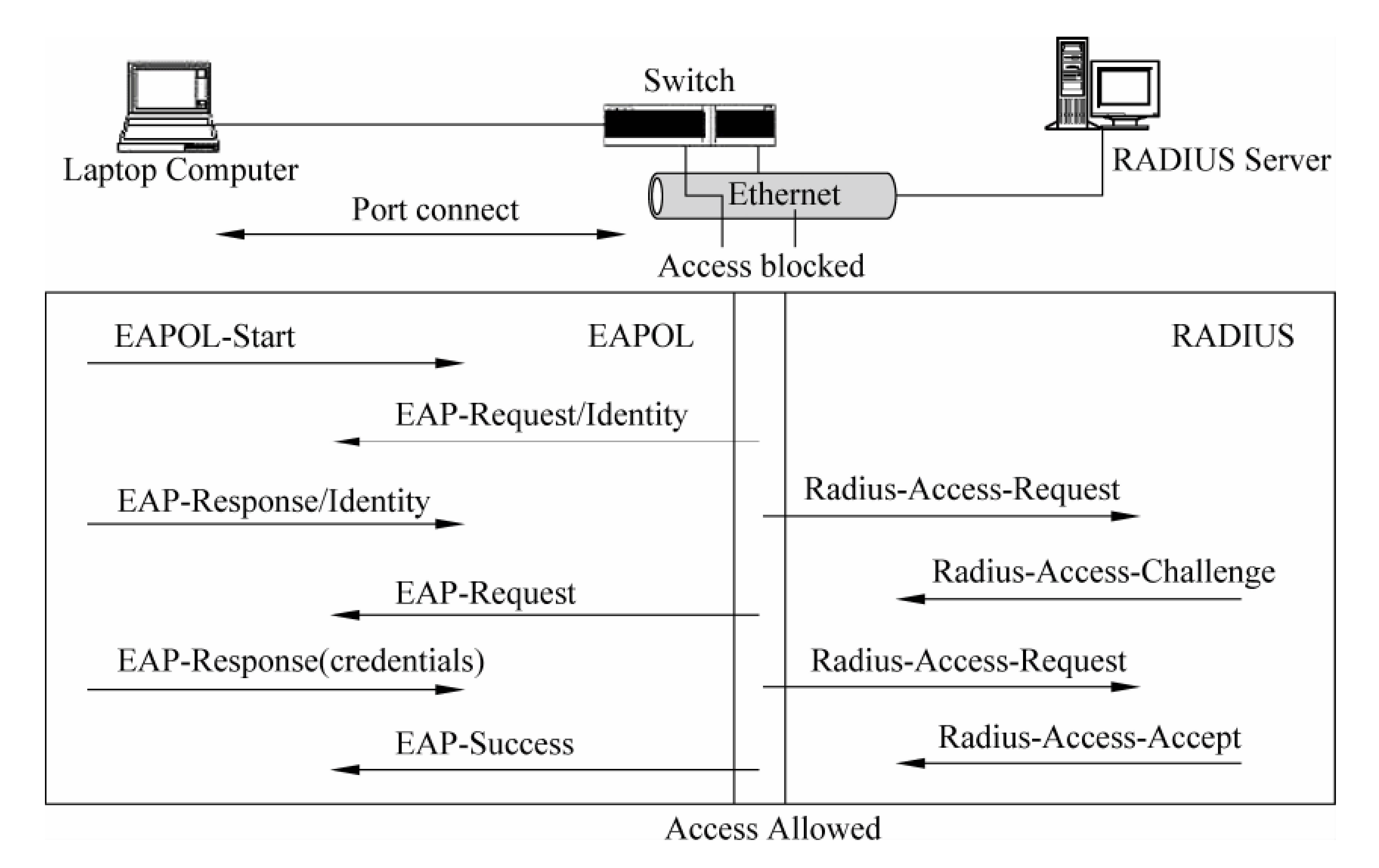


图 2-22 IEEE 802.1x 协议的状态

户计费。

⑧ 如果用户要下网，可以通过客户端软件发起 LogOff 过程，认证设备检测到该数据包后，会通知 AAA 服务器停止计费，并删除用户的相关信息(MAC/IP)，受控逻辑端口关闭。用户进入再认证状态。

⑨ 验证设备会通过定期检测来保证链路的激活，如果用户异常死机，则验证设备在发起多次检测后，自动认为用户已经下线，于是向认证服务器发送终止计费的信息。

(2) 无线网认证过程。

① 当一个移动结点(申请者)进入一个无线 AP 认证者的覆盖范围时，无线 AP 会向移动结点发出一个问询。

② 在收到来自 AP 的问询之后，移动结点做出响应，告知自己的身份。

③ AP 将移动结点的身份转发给 RADIUS 身份验证服务器，以便启动身份验证服务。

④ RADIUS 服务器请求移动结点发送它的凭据，并且指定确认移动结点身份所需凭据的类型。

⑤ 移动结点将它的凭据发送给 RADIUS。

⑥ 在对移动结点凭据的有效性进行确认之后，RADIUS 服务器将身份验证密钥发送给 AP。该身份验证密钥将被加密，只有 AP 能够读出该密钥。(在移动结点和 RADIUS 服务器之间传递的请求通过 AP 的“非控制”端口进行传递，因为移动结点不能直接与 RADIUS 服务器建立联系。AP 不允许 STA 移动结点通过“受控制”端口传送数据，因为它还没有经过身份验证。)

⑦ AP 使用从 RADIUS 服务器处获得的身份验证密钥保护移动结点数据的安全传输——特定于移动结点的单播会话密钥以及多播/全局身份验证密钥。

⑧ 全局身份验证密钥必须被加密。这要求所使用的 EAP 方法必须能够生成一个加密密钥，这也是身份验证过程的一个组成部分。传输层安全(Transport Level Security, TLS)协议提供了两点间的相互身份验证、完整性保护、密钥对协商以及密钥交换。可以使用 EAP-TLS，在 EAP 内部提供 TLS 机制。

移动结点可被要求周期性地重新认证，以保持一定的安全级。

5. 三种加密方式

(1) eap-md5。用户名与密码分开发送。RADIUS Server 给一个随机数，客户端使用这个随机数加密码，采用 MD5 算法得到一个真正的密码，最后送到 RADIUS Server，同时 RADIUS Server 也利用本身发的随机数加 Server 上的密码，采用 MD5 算法得到一个密码，与客户端发送过来的密码进行比较，如果一致，认证通过。流程图如图 2-23 所示。

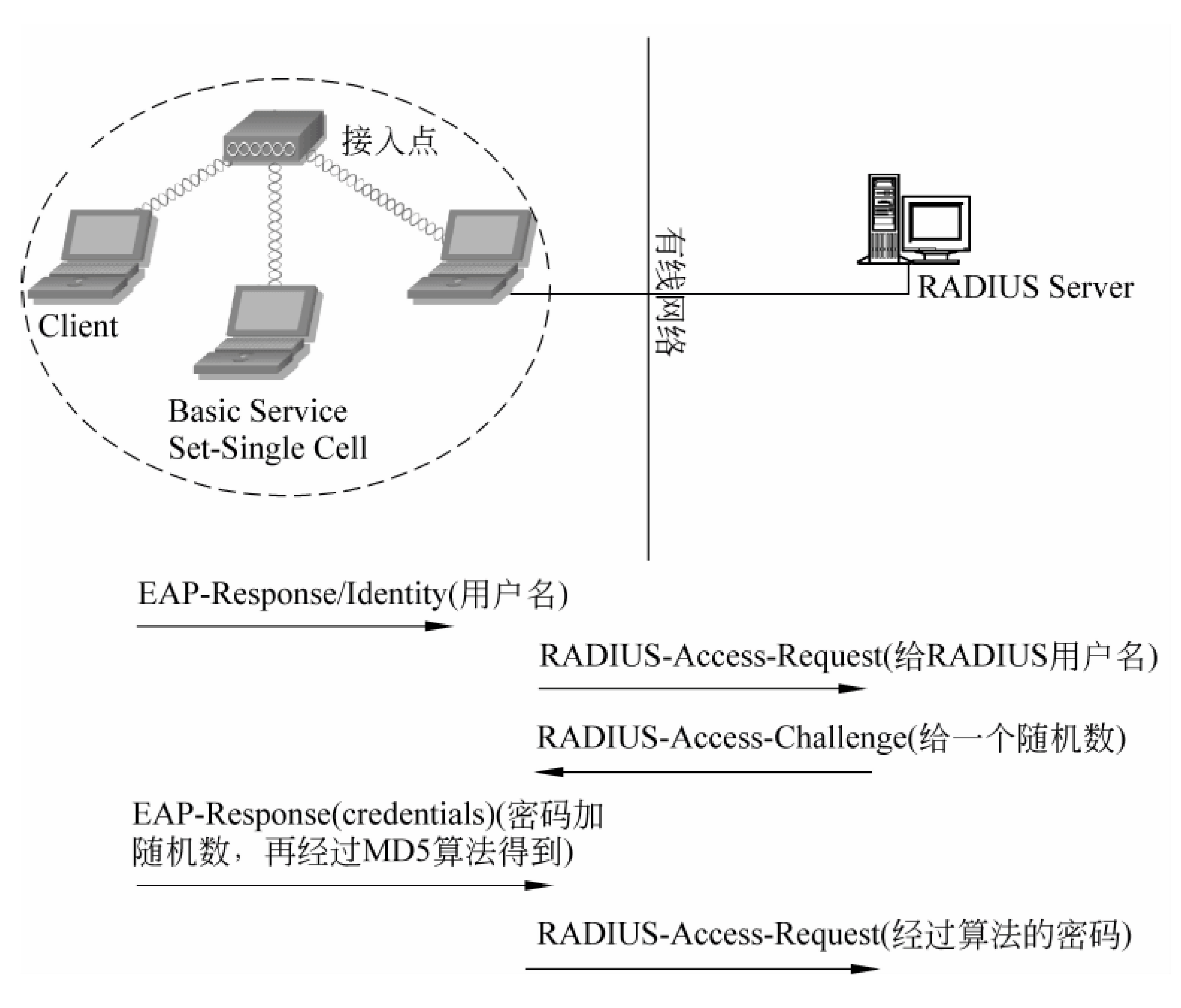


图 2-23　eap-md5 加密流程

(2) chap。用户名与密码是分开发送给交换机的，但发给 RADIUS Server 的只有一个 RADIUS-Access-Request，此请求包含了用户名、经过 MD5 算法的密码。算法中的随机数由交换机产生，交换机同时把此随机数发给客户端和 RADIUS Server。交换机与客户端的交互过程还是 6 次，但是和 RADIUS Server 的交换过程减少为 2 次。交换机等待到客户端的用户名、密码(经过算法以后的)后，才向 RADIUS Server 端发 RADIUS-Access-Request；RADIUS Server 根据交换机发过来的随机数再加上密码进行 MD5 算法，得到的结果来校核，确定是否认证通过。流程如图 2-24 所示。

(3) pap。与 chap 的发送过程一致，只是不使用 MD5 算法加密。

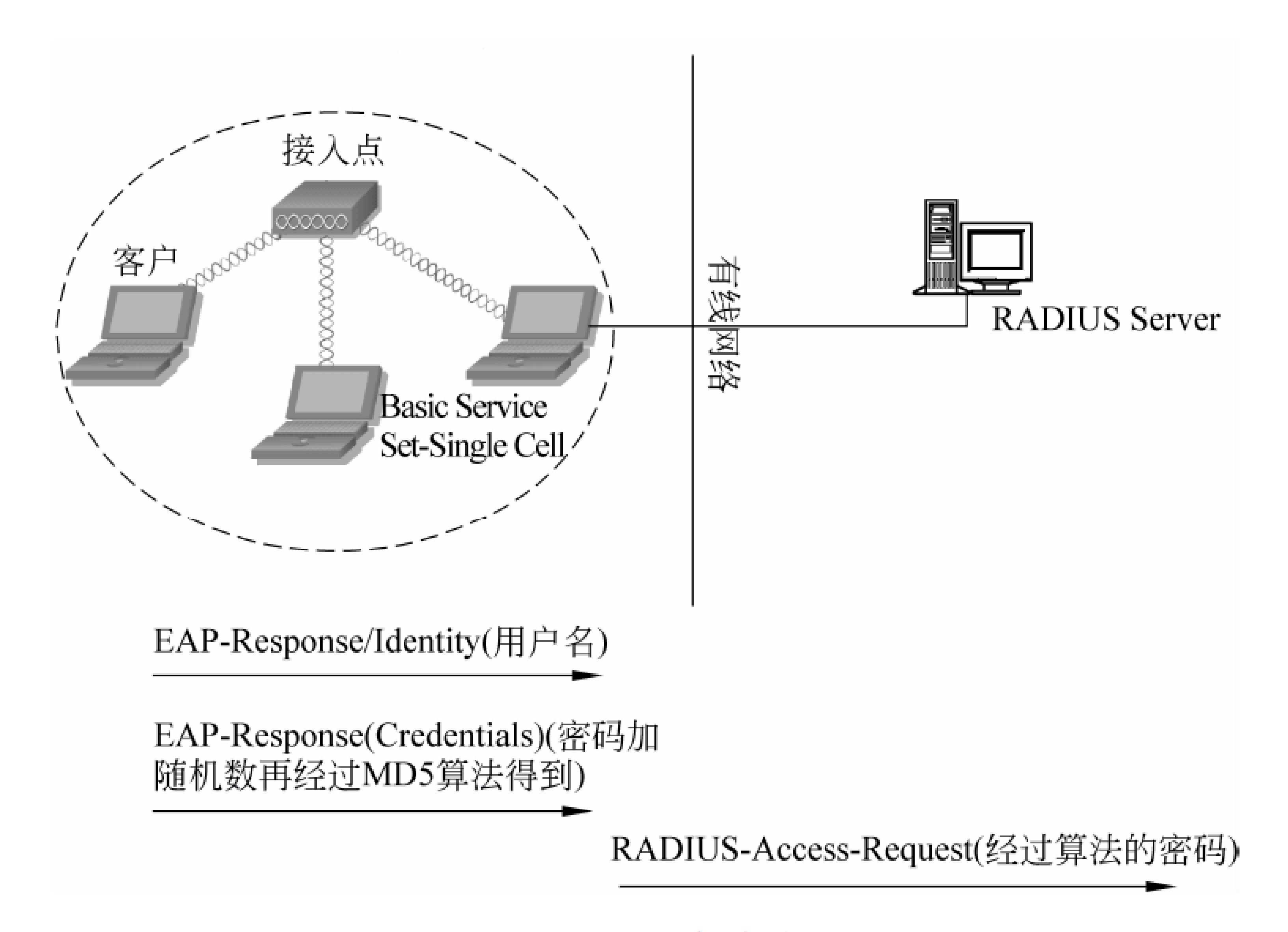


图 2-24　chap 加密流程

6. IEEE 802.1x 协议的特点

IEEE 802.1x 具有以下主要优点。

① 实现简单。IEEE 802.1x 协议为二层协议，不需要到达三层，对设备的整体性能要求不高，可以有效降低建网成本。

② 认证和业务数据分离。IEEE 802.1x 的认证体系结构中采用了“受控端口”和“非受控端口”的逻辑功能，从而可以实现业务与认证的分离。用户通过认证后，业务流和认证流实现分离，对后续的数据包处理没有特殊要求。业务可以很灵活，尤其在开展宽带组播等方面的业务有很大优势，所有业务都不受认证方式限制。

IEEE 802.1x 同时具有以下不足。

IEEE 802.1x 认证需要网络服务系统和网络之间的会话，它使用 IETF 的 EAP (Extensible Authentication Protocol) 认证协议。协议描述了认证机制的体系结构框架，使得能够在 IEEE 802.11 实体之间发送 EAP 包，并为在 AP 和工作站间的高层认证协议建立必要条件。对 MAC 地址的认证对 IEEE 802.1x 来说是最基本的，如果没有高层的每包认证机制，认证端口没有办法标识网络申请者。而且实验证明，IEEE 802.1x 由于设计缺陷，其安全性已经受到威胁，常见的攻击有中间人 MIM 攻击和会话攻击。

所以，IEEE 802.11 与 IEEE 802.1x 的简单结合并不能提供健壮的安全无线环境，必须由高层清晰的交互认证协议来加强。幸运的是，IEEE 802.1x 为实现高层认证提供了基本架构。

7. IEEE 802.1x 认证协议的应用

IEEE 802.1x 使用标准安全协议(如 RADIUS)提供集中的用户标识、身份验证、动态密钥管理和记账。IEEE 802.1x 身份验证可以增强安全性。IEEE 802.1x 身份验证提供

对 IEEE 802.11 无线网络和对有线以太网网络的经验证的访问权限。IEEE 802.1x 通过提供用户和计算机标识、集中的身份验证以及动态密钥管理，可将无线网络安全风险减小到最低程度。在此执行下，作为 RADIUS 客户端配置的无线接入点将连接请求和记账邮件发送到中央 RADIUS 服务器。中央 RADIUS 服务器处理此请求，并准予或拒绝连接请求。如果准予请求，根据所选身份验证方法，该客户端获得身份验证，并且为会话生成唯一密钥。IEEE 802.1x 为可扩展的身份验证协议 EAP 安全类型提供的支持使用户能够使用诸如智能卡、证书以及 Message Digest 5(MD5)算法这样的身份验证方法。

扩展身份验证协议 EAP 是一个支持身份验证信息通过多种机制进行通信的协议。利用 IEEE 802.1x，EAP 可以用来在申请者和身份验证服务器之间传递验证信息。这意味着 EAP 消息需要通过 LAN 介质直接封装。认证者负责在申请者和身份验证服务器之间传递消息。身份验证服务器可以是一台远程身份验证拨入用户服务(RADIUS)服务器。

以下例子说明对申请者进行身份验证所需经过的步骤。

① 认证者发送一个 EAP-Request/Identity(请求/身份)消息给申请者。

② 申请者发送一个 EAP-Response/Identity(响应/身份)以及它的身份给认证者。认证者将收到的消息转发给身份验证服务器。

③ 身份验证服务器利用一个包含口令问询的 EAP-Request 消息通过认证者对申请者做出响应。

④ 申请者通过认证者，将它对口令问询的响应发送给身份验证服务器。

⑤ 如果身份验证通过，授权服务器将通过认证者发送一个 EAP-Success 响应给申请者。认证者可以使用 Success(成功)响应，将受控制端口的状态设置为“已授权”。

8. 发展方向和趋势

IEEE 802.11 无线局域网目前的安全标准主要有两大发展主流方向。

(1) WPA。IEEE 802.1x 协议仅仅提供了一种用户接入认证的手段，并简单地通过控制接入端口的开/关状态来实现，这种简化适用于无线局域网的接入认证、点对点物理或逻辑端口的接入认证。WPA(Wi-Fi 受保护访问)是一种新的基于 IEEE 标准的安全解决方法。Wi-Fi 联盟经过努力，于 2002 年 10 月下旬宣布了基于此标准的解决方法，以便开发更加稳定的无线 LAN 安全解决方法，来满足 IEEE 802.11 的要求。WPA 包括 IEEE 802.1x 验证和 TKIP 加密(一种更高级和安全的 WEP 加密形式)，以进一步形成和完善 IEEE 802.11i 标准。

(2) WAPI。我国已于 2003 年 12 月 1 日起强制执行了新的无线局域网安全国家标准——无线局域网鉴别和保密基础结构(WLAN Authentication and Privacy Infrastructure，WAPI)，WAPI 由无线局域网鉴别基础结构(WLAN Authentication Infrastructure，WAI)和无线局域网保密基础结构(WLAN Privacy Infrastructure，WPI)组成。与已有安全机制相比，WAPI 具有独特优点，充分体现了国家标准的先进性，在很多方面都进行了改进。它已由 ISO/IEC 授权的 IEEE Registration Authority 审查获得认可，分配了用于 WAPI 协议的以太网类型字段，这也是我国目前在该领域唯一获得批准的协议。WAPI 采用国家密码管理委

员会办公室批准的公开密钥体制的椭圆曲线密码算法和秘密密钥体制的分组密码算法，分别用于 WLAN 设备的数字证书、密钥协商和传输数据的加解密，从而实现设备的身份鉴别、链路验证、访问控制和用户信息在无线传输状态下的加密保护。

习题 2

一、填空题

1. 数据链路层安全性是指在数据链路上各个结点之间能够安全地交换数据，它表现为保障数据的________和________两个方面。

2. PPTP 协议采用一种增强的________协议来封装 PPP 数据包。

3. PPTP 协议提供了两种用户身份认证方式，它们分别为________和________。

二、选择题

1. PPTP 的一个弱点就是它依赖于 PPP。在进行任何通信之前，由 PPP 建立和初始化通信参数，因为 PPP 没有对这些分组进行认证，可能发生________。

A. 密钥管理攻击　　B. 中间人攻击
C. 拒绝服务攻击　　D. 回放攻击

2. L2TP 隧道在两端的 VPN 服务器之间采用________ 来验证对方的身份。

A. 口令握手协议　　B. SSL
C. Kerberos　　D. 数字证书

3. PPTP 的加密方法采用________算法，可以选用较弱的 40 位密钥或强度较大的 128 位密钥。

A. DES　　B. MPPE
C. RSA　　D. AES

三、判断题

IEEE 802.10 协议最初是制定一个互操作的局域网安全标准，后来作为 VLAN 标识符。(　　)

四、思考题

1. PPTP 的目的是要解决什么问题?

2. PPTP 提供了哪些安全机制?

3. PPTP 存在哪些安全隐患?

第 3 章　网络层安全协议

IP 网络安全一直是一个备受关注的领域，如果缺乏一定的安全保障，无论是公共网络还是企业专用网络，都难以抵挡网络攻击和非法入侵。对于某个特定的企业内部网 Intranet 来说，网络攻击既可能来自网络内部，也可能来自外部的 Internet，其结果均可能导致企业内部网络毫无安全性可言，单靠口令访问控制不足以保证数据在网络传输过程中的安全性。

3.1　网络攻击与防御

3.1.1　常见的网络攻击

如果没有适当的安全措施和安全的访问控制方法，在网络上传输的数据很容易受到各式各样的攻击。网络攻击既有被动型的，也有主动型的。被动攻击通常指信息受到非法侦听，而主动攻击则往往意味着对数据甚至网络本身恶意的篡改和破坏。以下列举几种常见的网络攻击类型。

1. 窃听

一般情况下，绝大多数网络通信都以一种不安全的“明文”形式进行，这就给攻击者很大的机会。只要获取数据通信路径，就可轻易“侦听”或者“解读”明文数据流。窃听型攻击者虽然不破坏数据，却可能造成通信信息外泄，甚至危及敏感数据安全。对于多数普通企业来说，这类网络窃听行为已经构成网管员面临的最大的网络安全问题。

2. 数据篡改

网络攻击者非法读取数据后，下一步通常就想去篡改它，而且这种篡改一般可以做得让数据包的发送方和接收方无知无觉。但作为网络通信用户，即使并非所有的通信数据都是高度机密的，也不想看到数据在传输过程中出现任何差错。比如在网上购物，一旦我们提交了购物订单，谁也不希望订单中的任何内容被人肆意篡改。

3. 身份欺骗(IP 地址欺骗)

大多数网络操作系统使用 IP 地址来标识网络主机。然而，一些貌似合法的 IP 地址很有可能是经过伪装的，这就是所谓的 IP 地址欺骗，也就是身份欺骗。另外，网络攻击者还可以使用一些特殊的程序，对某个从合法地址传来的数据包做些手脚，借此合法地址来非法侵入某个目标网络。

4. 盗用口令攻击(Password-Based Attack)

基于口令的访问控制是一种最常见的安全措施。这意味着对某台主机或网络资源的访问权限决定于谁,也就是说,这种访问权是基于用户名和账号密码的。

攻击者可以通过多种途径获取用户合法账号,一旦拥有了合法账号,也就拥有了与合法用户同等的网络访问权限。因此,假设账号被盗的用户具有网管权限,攻击者甚至可以借机给自己再创建一个合法账号,以备后用。有了合法账号进入目标网络后,攻击者也就可以随心所欲地盗取合法用户信息以及网络信息;修改服务器和网络配置,包括访问控制方式和路由表;篡改、重定向、删除数据等。

5. 拒绝服务攻击(Denial-of-Service Attack)

与盗用口令攻击不同,拒绝服务攻击的目的不在于窃取信息,而是要使某个设备或网络无法正常运作。在非法侵入目标网络后,这类攻击者惯用的攻击手法如下。

(1) 首先设法转移网管员注意力,使之无法立刻察觉有人入侵,从而给自己争取时间。

(2) 向某个应用系统或网络服务系统发送非法指令,致使系统出现异常行为或异常终止。

(3) 向某台主机或整个网络发送大量数据洪流,导致网络因不堪过载而瘫痪。

(4) 拦截数据流,使授权用户无法取得网络资源。

6. 中间人攻击(Man-in-the-Middle Attack)

顾名思义,中间人攻击发生在用户与通信对象之间,即通信过程以及通信数据遭到第三方的监视、截取和控制,例如攻击者可以对数据交换进行重定向等。如果通信中使用网络底层协议,通信两端的主机是很难区分出不同对象的,因此也不大容易察觉这类攻击。中间人攻击有点类似于身份欺骗。

7. 盗取密钥攻击(Compromised-Key Attack)

一般来说,盗取密钥是很困难的,但并非不可能。通常把被攻击者盗取的密钥称为“已泄密的密钥”。攻击者可以利用这个已泄密的密钥,对数据进行解密和修改,甚至还能试图利用该密钥计算其他密钥,以获取更多加密信息。

3.1.2 防御方法及优点

1. 边界防御

众所周知,网络攻击常常可能导致系统崩溃及敏感数据的外泄,因此数据资源必须受到足够的保护,以防被侦听、篡改或非法访问。

常规网络保护策略有使用防火墙、安全路由器(安全网关)以及对拨号用户进行身份

认证等。这些措施通常被称为“边界保护”,往往只着重于抵御来自网络外部的攻击,但不能阻止网络内部的攻击行为。例如,一台主机由多个用户共享,往往会发生人不在了,而机器却仍处于登录状态的情况,从而导致系统出现不安全因素。访问控制法最大的缺陷是一旦用户账号被窃,就根本无法阻止攻击者盗取网络资源。

还有一种比较少见的保护策略是物理级保护,就是保护实际的网络线路和网络访问结点,禁止任何未经授权的使用。但采用这种保护方式,当数据需要从数据源通过网络传输到目的地时,无法做到保证数据的全程安全。

2. 用 IPSec 抵御网络攻击

IPSec 采用端到端加密模式,基本工作原理是发送方在数据传输前(即到达网线之前)对数据实施加密。在整个传输过程中,报文都是以密文方式传输,直到数据到达目的结点,才由接收端进行解密。IPSec 对数据的加密以数据包而不是整个数据流为单位,这不仅更灵活,也有助于进一步提高 IP 数据包的安全性。通过提供强有力的加密保护,IPSec 可以有效防范网络攻击,保证专用数据在公共网络环境下的安全性。

一个完善的企业安全计划,应该是多种安全策略的有机组合,将 IPSec 与用户访问控制、边界保护以及物理层保护相结合,可以为企业数据通信提供更高层次的纵深防护。网络攻击者要破译经过 IPSec 加密的数据,即使不是完全不可能,也是非常困难的。根据不同类别数据的不同保密需求,IPSec 策略中有多种等级的安全强度可供选择,使用 IPSec 可以显著地减少或防范前面谈到的几种网络攻击。

(1) 窃听。Sniffer 可以读取数据包中的任何信息,因此对抗窃听最有效的方法就是对数据进行加密。IPSec 的封装安全载荷 ESP 协议通过对 IP 包进行加密来保证数据的私密性 。

(2) 数据篡改。IPSec 用密钥为每个 IP 包生成一个检查和,该密钥为且仅为数据的发送方和接收方共享。对数据包的任何篡改都会改变检查和,从而让接收方得知包在传输过程中遭到了修改。

(3) 身份欺骗,盗用口令,应用层攻击。IPSec 的身份交换和认证机制不会暴露任何信息,不给攻击者可乘之机,双向认证在通信系统之间建立信任关系,只有可信赖的系统才能彼此通信。

(4) 中间人攻击。IPSec 结合双向认证和共享密钥,足以抵御中间人攻击。

(5) 拒绝服务攻击。IPSec 使用 IP 包过滤法,依据 IP 地址范围、协议甚至特定的协议端口号来决定哪些数据流需要受到保护,哪些数据流可以被允许通过,哪些需要拦截。

3. 第三层保护的优点

通常,IPSec 提供的保护需要对系统作一定修改,但是 IPSec 在 IP 传输层,即第三层的“策略执行”(Strategic Implementation),几乎不需要什么额外开销就可以实现为绝大多数应用系统、服务和上层协议提供较高级别的保护;为现有的应用系统和操作系统配置,IPSec 几乎无须作任何修改,安全策略可以在 Active Directory 里集中定义,也可以在某台主机上进行本地化管理。

IPSec 策略在 ISO 参考模型第三层即网络层上实施的安全保护，范围几乎涵盖了 TCP/IP 协议族中所有 IP 协议和上层协议，如 TCP、UDP、ICMP、Raw(第 255 号协议)，甚至包括在网络层发送数据的客户自定义协议。在第三层上提供数据安全保护的主要优点就在于所有使用 IP 协议进行数据传输的应用系统和服务都可以使用 IPSec，而不必对这些应用系统和服务本身作任何修改。

运作于第三层以上的其他一些安全机制，如安全套接层 SSL，仅对知道如何使用 SSL 的应用系统(如 Web 浏览器)提供保护，这极大地限制了 SSL 的应用范围；而运作于第三层以下的安全机制，如链路层加密，通常只保护了特定链路间的数据传输，而无法做到在数据路径所经过的所有链路间提供安全保护，这使得链接层加密无法适用于 Internet 或路由 Intranet 方案中的端对端数据保护。

3.2 IPSec 体系结构

3.2.1 IPSec 体系结构

IPSec (Internet 协议安全)是一个工业标准网络安全协议，为 IP 网络通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，可以有效抵御网络攻击，同时保持易用性。IPSec 有两个基本目标：

① 保护 IP 数据包安全；

② 为抵御网络攻击提供防护措施。

IPSec 基于一种端到端的安全模式。这种模式有一个基本前提假设，就是假定数据通信的传输媒介是不安全的，因此通信数据必须经过加密。而掌握加解密方法的只有数据流的发送端和接收端，两者各自负责相应的数据加解密处理，而网络中其他只负责转发数据的路由器或主机无须支持 IPSec。该特性有助于企业用户在下列方案中成功地配置 IPSec。

(1) 局域网：C/S 模式，对等模式。

(2) 广域网：路由器到路由器模式，网关到网关模式。

(3) 远程访问：拨号客户机，专网对 Internet 的访问。

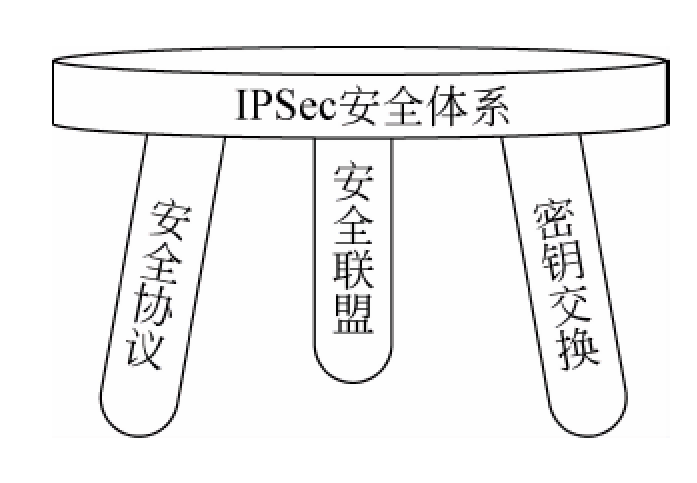


图 3-1 IPSec 组成结构

IPSec 结合安全联盟、安全协议组和动态密钥管理三者来实现上述两个目标，如图 3-1 所示，不仅能为企业局域网与拨号用户、域、网站、远程站点以及 Extranet 之间的通信提供强有力且灵活的保护，而且还能用来筛选特定数据流。

IPSec(IP Security)协议是 IETF 安全工作组制定的一套可以用于 IPv4 和 IPv6 上的、具有互操作性的、基于密码学的安全协议。IPv4 可选支持 IPSec，IPv6 必须支持 IPSec。IPSec 提供的安全服务包括访问控制、无连接的完整性、数据源头的认证、防重放功能、数据保密和一定的数据流保密等。IPSec 协议产生的初衷是解决 Internet 上 IP 传输的安全性问题，它包括从 RFC 2401 到 RFC 2412 的一系列 RFC，定义了一套默认的、

强制实施的算法,以保证不同的实施方案可以互通。IPSec 标准包含了 IP 安全体系结构、IP 认证 AH 头、IP 封装安全载荷 ESP 和 Internet 密钥交换(IKE)4 个核心的基本规范,组成了一个完整的安全体系结构,如图 3-2 所示。

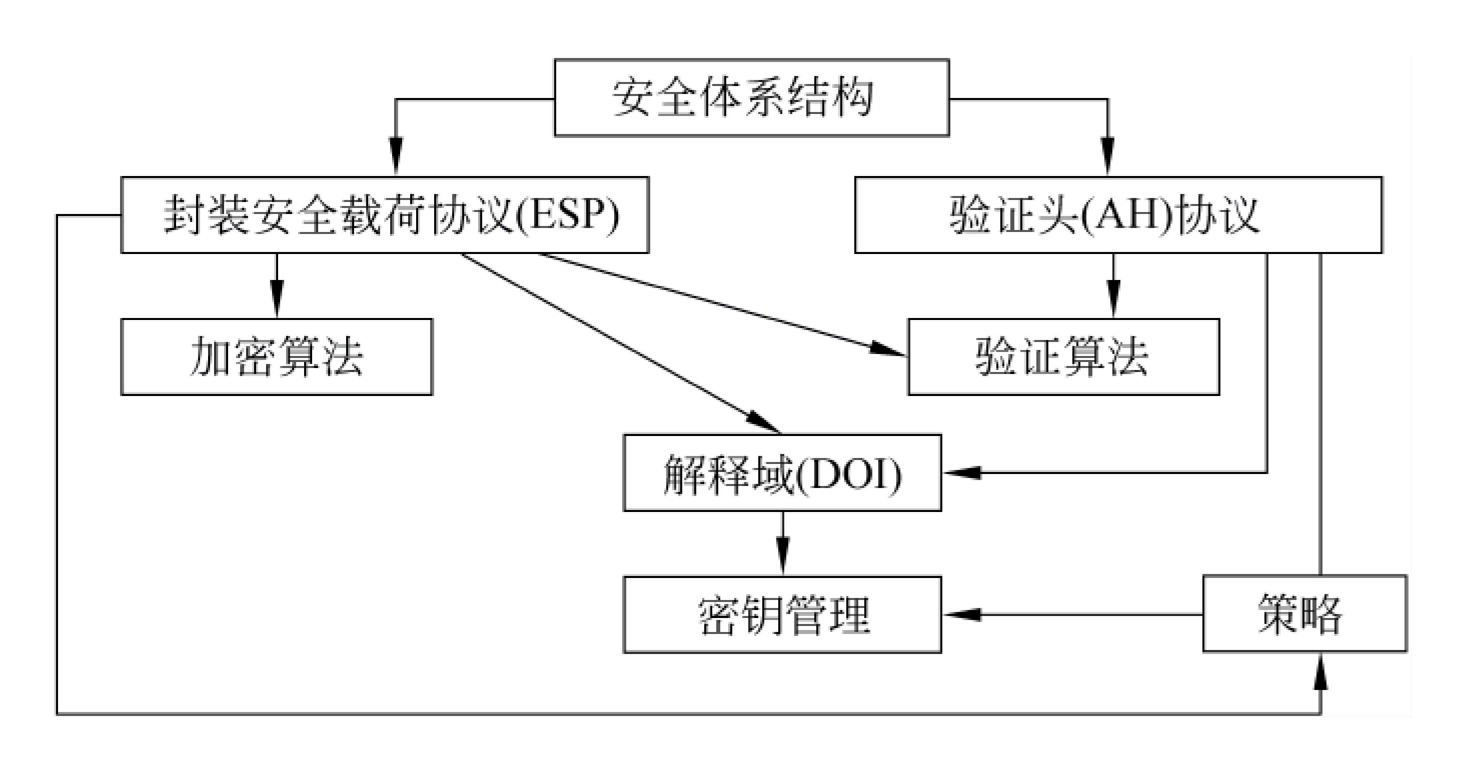


图 3-2 IPSec 安全体系结构

(1) 安全体系结构。包含一般的概念、安全需求和定义 IPSec 的技术机制。

(2) ESP 协议。加密 IP 数据包的默认值、头部格式以及与加密封装相关的其他条款。

(3) AH 协议。验证 IP 数据包的默认值、头部格式以及与认证相关的其他条款。

(4) 加密算法。描述各种加密算法如何用于 ESP 中。

(5) 验证算法。描述各种身份验证算法如何用于 AH 和 ESP 身份验证选项。

(6) 密钥管理。描述因特网 IETF 标准密钥管理方案。其中 IKE 是默认的密钥自动交换协议。

(7) 解释域 DOI。是因特网统一协议参数分配权威机构(Internet Assigned Number Authority,IANA)中数字分配机制的一部分,它描述的值是预知的。包括彼此相关各部分的标志符及运作参数。

(8) 策略。决定两个实体之间能否通信,以及如何进行通信。策略的核心由三部分组成:SA、SAD、SPD。SA(安全关联)表示了策略实施的具体细节,包括源/目的地址、应用协议、SPI(安全策略索引)等;SAD 为进入和外出包处理维持一个活动的 SA 列表;SPD 决定了整个 VPN 的安全需求。策略部分是唯一尚未成为标准的部件。

3.2.2 IPSec 驱动程序

1. IPSec 驱动程序

IPSec 驱动程序负责监视、筛选和 IP 通信。它负责监视所有出入站的 IP 数据包,并将每个 IP 数据包与作为 IP 策略一部分的 IP 筛选器相匹配。一旦匹配成功,IPSec 驱动程序通知 IKE 开始协商,图 3-3 为 IPSec 驱动程序服务示意图。

协商成功完成后,发送端 IPSec 驱动程序执行以下步骤。

(1) 从 IKE 处获得 SA 和会话密钥。

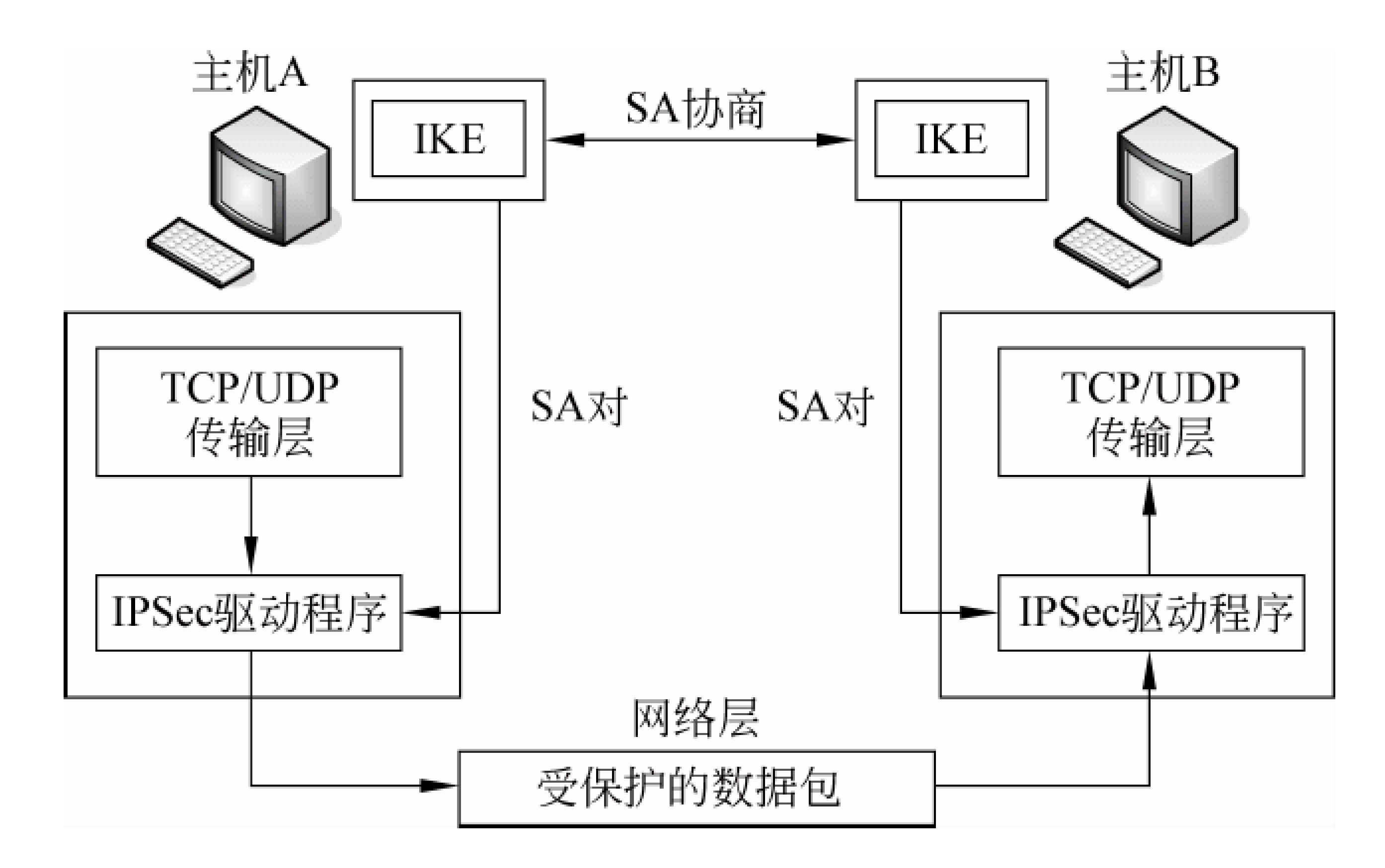


图 3-3　IPSec 驱动程序服务示意图

(2) 在 IPSec 驱动程序数据库中查找相匹配的出站 SA，并将 SA 中的 SPI 插入 IPSec 包头。

(3) 对数据包签名(完整性检查)；如果要求机密，则另外加密数据包。

(4) 将数据包随同 SPI 发送 IP 层，然后进一步转发至目的主机。

接收端 IPSec 驱动程序执行以下步骤。

(1) 从 IKE 处获得会话密钥，SA 和 SPI。

(2) 通过目的地址和 SPI，在 IPSec 驱动程序数据库中查找相匹配的入站 SA。

(3) 检查签名，对数据包进行解密(如果是加密包的话)。

(4) 将数据包递交给 TCP/IP 驱动程序，然后再交给接收应用程序。

2. IPSec 工作流程

IPSec 的流程如下所述，为简单起见，本书假设这是一个 Intranet 例子，每台主机都有处于激活状态的 IPSec 策略。

(1) 用户甲(在主机 A 上)向用户乙(在主机 B 上)发送一消息。

(2) 主机 A 上的 IPSec 驱动程序检查 IP 筛选器，查看数据包是否需要以及需要受到何种保护。

(3) 驱动程序通知 IKE 开始协商。

(4) 主机 B 上的 IKE 收到请求协商通知。

(5) 两台主机建立第一阶段 SA，各自生成共享“主密钥”。若两机在此前通信中已经建立起第一阶段 SA，则可直接进行第二阶段 SA 协商。

(6) 协商建立第二阶段 SA 对：入站 SA 和出站 SA。SA 包括密钥和 SPI。

(7) 主机 A 上的 IPSec 驱动程序使用出站 SA，对数据包进行签名(完整性检查)与加密。

(8) 驱动程序将数据包递交 IP 层，再由 IP 层将数据包转发至主机 B。

(9) 主机 B 网络适配器驱动程序收到数据包并提交给 IPSec 驱动程序。

(10) 主机 B 上的 IPSec 驱动程序使用入站 SA，检查签名完整性并对数据包进行

解密。

(11) 驱动程序将解密后的数据包提交上层 TCP/IP 驱动程序,再由 TCP/IP 驱动程序将数据包提交主机 B 的接收应用程序。

以上是 IPSec 的一个完整工作流程,虽然看起来很复杂,但所有操作对用户是完全透明的。中介路由器或转发器仅负责数据包的转发,如果中途遇到防火墙、路由器或代理服务器,则要求它们具有 IP 转发功能,以确保 IPSec 和 IKE 数据流不会遭拒绝。

这里需要指出的是,使用 IPSec 的数据包不能通过网络地址译码 NAT。因为 IKE 协商中所携带的 IP 地址是不能被 NAT 改变的,对地址的任何修改都会导致完整性检查失效。

3.2.3 IPSec 采用的安全技术

1. IPSec 的安全特性

IPSec 有两个基本安全目标,决定它应该拥有以下 5 个安全特性。

(1) 不可否认性。"不可否认性"可以证实消息发送方是唯一可能的发送者,发送者不能否认发送过消息。"不可否认性"是采用公钥技术的一个特征,当使用公钥技术时,发送方用私钥产生一个数字签名,随消息一起发送,接收方用发送者的公钥来验证数字签名。在理论上,只有发送者才唯一拥有私钥;"不可否认性"不是基于认证的共享密钥技术的特征,因为在基于认证的共享密钥技术中,发送方和接收方掌握相同的密钥。

(2) 反重播性。"反重播"确保每个 IP 包的唯一性,保证信息万一被截取复制后,不能再被重新利用、重新传输回目的地址。该特性可以防止攻击者截取破译信息,再用相同的信息包冒取非法访问权(即使这种冒取行为发生在数月之后)。

(3) 数据完整性。防止传输过程中数据被篡改,确保发出数据和接收数据的一致性。IPSec 利用 Hash 函数,为每个数据包产生一个加密检查和,接收方在打开包前,先计算检查和,若包遭篡改导致检查和不相符,数据包即被丢弃。

(4) 数据可靠性(加密)。传输前对数据进行加密,可以保证即使传输过程中数据包遭截取,信息也无法被读。该特性在 IPSec 中为可选项,与 IPSec 策略的具体设置相关。

(5) 认证。数据源发送信任状,由接收方验证信任状的合法性,只有通过认证的系统才可以建立通信连接。

2. 基于电子证书的公钥认证

一个架构良好的公钥体系,在信任状的传递中不造成任何信息外泄,能解决很多安全问题。IPSec 与特定的公钥体系相结合,可以提供基于电子证书的认证。公钥证书认证在 Windows 2000 中,适用于对非 Windows 2000 主机、独立主机、非信任域成员的客户机或者不运行 Kerberos v5 认证协议的主机进行身份认证。

3. 预置共享密钥认证

IPSec 也可以使用预置共享密钥进行认证。预共享意味着通信双方必须在 IPSec 策

略设置中就共享的密钥达成一致。之后，在安全协商过程中，信息在传输前使用共享密钥加密，接收端使用同样的密钥解密。如果接收方能够解密，即被认为可以通过认证。但在Windows 2000 IPSec 策略中，这种认证方式被认为不够安全，而一般不推荐使用。

4. 公钥加密

IPSec 的公钥加密用于身份认证和密钥交换。使用公钥加密法，每个用户拥有一个密钥对，其中私钥仅为个人所知，公钥则可分发给任意需要与之进行加密通信的人。例如：A 想要发送加密信息给 B，则 A 需要用 B 的公钥加密信息，之后只有 B 才能用他的私钥解密该加密信息。虽然密钥对中两把钥匙彼此相关，但要想从其中一把推导出另一把，以目前计算机的运算能力来看，这种做法非常困难。因此，在这种加密法中，公钥可以广为分发，而私钥则需要仔细地妥善保管。

5. Hash 函数保证数据完整性

Hash 信息验证码(Hash Message Authentication Codes，HMAC)验证接收消息和发送消息的完全一致性(完整性)。这在数据交换中非常关键，尤其当传输媒介，如公共网络中不提供安全保证时更显重要。

HMAC 结合 Hash 算法和共享密钥提供完整性。Hash 散列通常也被当成是数字签名，但这种说法不够准确，两者的区别在于：Hash 散列使用共享密钥，而数字签名基于公钥技术。Hash 算法也称为消息摘要或单向转换。称它为单向转换的原因如下。

(1) 双方必须在通信的两端各自执行 Hash 函数计算。

(2) 使用 Hash 函数很容易从消息计算出消息摘要，但以目前计算机的运算能力，其逆向反演过程几乎不可实现。

Hash 散列本身就是所谓加密检查和或消息完整性编码(Message Integrity Code，MIC)，通信双方必须各自执行函数计算来验证消息。举例来说，发送方首先使用 HMAC 算法和共享密钥计算消息检查和，然后将计算结果 A 封装进数据包中一起发送；接收方再对所接收的消息执行 HMAC 计算得出结果 B，并将 B 与 A 进行比较。如果消息在传输中遭篡改，致使 B 与 A 不一致，接收方丢弃该数据包。

有两种最常用的 Hash 函数，内容如下。

(1) HMAC-MD5。MD5(消息摘要 5)基于 RFC 1321。MD5 对 MD4 做了改进，计算速度比 MD4 稍慢，但安全性能得到了进一步改善。MD5 在计算中使用了 64 个 32 位常数，最终生成一个 128 位的完整性检查和。

(2) HMAC-SHA。安全 Hash 算法定义在 NIST FIPS 180-1，其算法以 MD5 为原型。SHA 在计算中使用了 79 个 32 位常数，最终产生一个 160 位完整性检查和。SHA 检查和长度比 MD5 更长，因此安全性也更高。

6. 加密保证数据可靠性

IPSec 使用的数据加密算法是 DES-Data Encryption Standard(数据加密标准)。DES 密钥长度为 56 位，在形式上是一个 64 位数。DES 以 64 位(8 字节)为分组对数据加

密，每64位明文，经过16轮置换生成64位密文，其中每字节有1位用于奇偶校验，所以实际有效密钥长度是56位。IPSec还支持3DES算法，3DES可提供更高的安全性，但计算速度更慢。

7. 密钥管理

(1) 动态密钥更新。IPSec策略使用"动态密钥更新"法决定一次通信中新密钥产生的频率。在通信过程中，动态密钥指数据流被划分成一个个"数据块"，每一个"数据块"都使用不同的密钥加密，这可以保证万一攻击者中途截取了部分通信数据流和相应的密钥后，也不会危及到其余通信信息的安全。动态密钥更新服务由Internet密钥交换(Internet Key Exchange，IKE)提供，详见IKE介绍部分。

IPSec策略允许专家级用户自定义密钥生命周期。如果该值没有设置，则按默认时间间隔自动生成新密钥。

(2) 密钥长度。密钥长度每增加一位，可能的密钥数就会增加一倍，相应地，破解密钥的难度也会随之呈指数级加大。IPSec策略提供多种加密算法，可生成多种长度不等的密钥，用户可根据不同的安全需求加以选择。

(3) Diffie-Hellman算法。要启动安全通信，通信两端必须首先得到相同的共享密钥(主密钥)，但共享密钥不能通过网络相互发送，因为这种做法极易泄密。

Diffie-Hellman算法是用于密钥交换的最早最安全的算法之一。DH算法的基本工作原理如下：通信双方公开或半公开交换一些准备用来生成密钥的"素材数据"，彼此交换过密钥生成"素材"后，两端可以各自生成出完全一样的共享密钥。在任何时候，双方都绝不交换真正的密钥。

通信双方交换的密钥生成"素材"，长度不等，"素材"长度越长，所生成的密钥强度也就越高，密钥破译就越困难。除进行密钥交换外，IPSec还使用DH算法生成所有其他加密密钥。

3.3 IPSec安全协议

IPSec在IP层提供安全服务，它使系统能按需选择安全协议，决定服务所使用的算法及放置需求服务所需密钥到相应位置。IPSec用来保护一条或多条主机与主机间、安全网关与安全网关间、安全网关与主机间的路径。

IPSec能提供的安全服务集包括访问控制、无连接的完整性、数据源认证、拒绝重发包(部分序列完整性形式)、保密性和有限传输流保密性。因为这些服务均在IP层提供，所以任何高层协议均能使用它们，例如TCP、UDP、ICMP、BGP等。

这些目标是通过使用两大传输安全协议，头部认证(AH)和封装安全负载(ESP)以及密钥管理程序和协议的使用来完成的。所需的IPSec协议集内容及其使用方式是由用户、应用程序和/或站点、组织对安全和系统的需求来决定。

IPSec结构包括众多协议和算法，这些协议之间的相互关系如图3-2所示。由图可知，IPSec协议不是一个单独的协议，它给出了应用于IP层上网络数据安全的一整套体

系结构，包括网络认证协议 Authentication Header（AH）、封装安全载荷协议（Encapsulating Security Payload，ESP）、密钥管理协议（Internet Key Exchange，IKE）和用于网络认证及加密的一些算法等。IPSec 规定了如何在对等层之间选择安全协议、确定安全算法和密钥交换，向上提供访问控制、数据源认证、数据加密等网络安全服务。

IPSec 提供了两种机制：认证和加密。认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份，以及数据在传输过程中是否遭篡改。加密机制通过对数据进行编码来保证数据的机密性，以防数据在传输过程中被窃听。其中，AH 协议定义了认证的应用方法，提供数据源认证和完整性保证；ESP 协议定义了加密和可选认证的应用方法，提供可靠性保证。在实际进行 IP 通信时，可以根据实际需求同时使用这两种协议或选择使用其中的一种。AH 和 ESP 都可以提供认证服务，不过，AH 提供的认证服务要强于 ESP。

3.3.1 Authentication Header 协议

1. Authentication Header 协议结构

Authentication Header（AH）协议主要提供认证机制，保证数据包接收者得到的源地址是可靠的，同时也提供了数据的完整性，抗重播攻击的能力。它使通信免受篡改，但不能防止窃听，适合用于传输非机密数据。

AH 的工作原理是在每一个数据包上添加一个身份验证包头。此包头包含一个带密钥的 Hash 散列（可以将其当做数字签名，只是它不使用证书），此 Hash 散列在整个数据包中计算，因此对数据的任何更改将致使散列无效，提供对数据的完整性保护。

AH 包头位置在 IP 包头和传输层协议包头之间，如图 3-4 所示。AH 由 IP 协议号“51”标识，该值包含在 AH 包头之前的协议包头中，如 IP 包头。AH 可以单独使用，也可以与 ESP 协议结合使用。

IP包头	AH包头	TCP包头	数据

验证（←——→）

图 3-4　AH 为整个数据包提供完整性检查

AH 由 5 个固定长度域和一个变长的认证数据域组成，如图 3-5 所示。

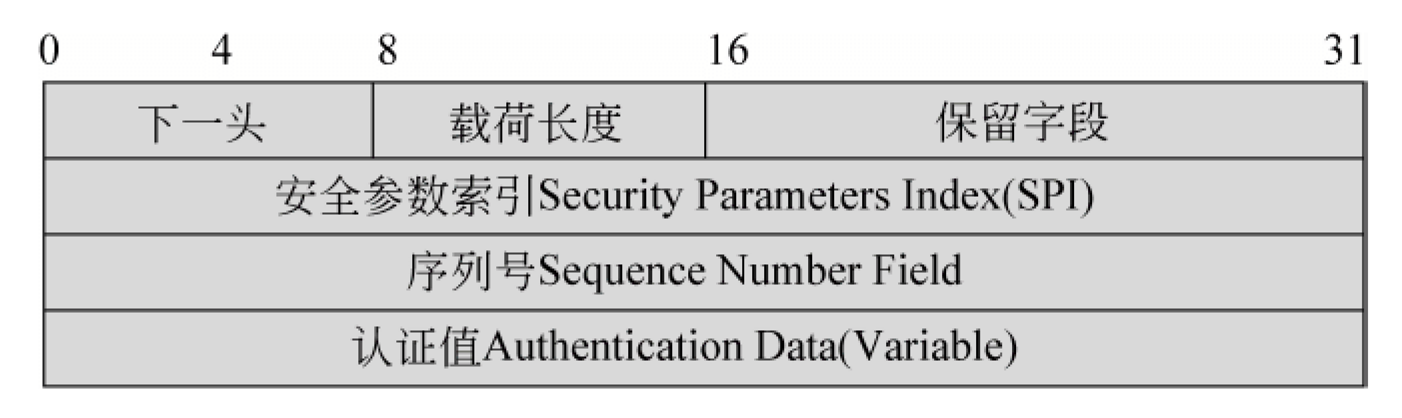


图 3-5　AH 包头格式

其中的字段意义如下。

（1）下一头：（8 位），识别这个包头之后紧跟的包头类型。在传输模式下，表示处于保护中的上层协议的值，比如 TCP 或 UDP 的值。

(2) 载荷长度:(8位),其值等于AH头长度(以32位字长计算)减去2。AH头是一个IPv6的扩展头,按照RFC 2460标准的规定,它的值是头长度减去一个64位,在认证数据为标准的96位时,这个域的值为4。

(3) 保留字段:16位,该字段用于今后的扩充,设置为0。

(4) 安全参数索引SPI:专有32位值,用以区分那些目的IP地址和安全协议类型相同,但算法不同的数据包。它与数据包的目的IP地址、安全协议类型(AH)一起,唯一确定了这一数据包所用的安全关联SA。SPI的值在SA建立时由目的主机确定,如果一个新的SA尚未建立好,即它的密钥还在通信双方协商之时,该SA内部的SPI值要取为0。

(5) 序列号:32位整数,它代表一个单调递增计数器的值。即使接收方不使用"抗重放攻击"功能时,发送方也一定要发送这一序列号。是否处理序列号,取决于接收方,即发送方总是传送序列号,但接收方不必强制性处理它。当SA建立时,发送方和接收方的序列号值被初始化为0。通信双方每使用一个特定的SA发出一个数据包,就将他们的相应序列号加1。如果使用"抗重放"功能,计数不能循环,即让计数器值变成0。在计数快接近溢出时(2的12次方),通信双方应重新协商,建立一个新的SA及新的密钥。

(6) 认证值:这个域的长度可变,它存放IP数据包的完整性校验值ICV。ICV是消息身份验证码或是由MAC算法产生的代码删节。对于IPv4数据包,认证数据一定要为整数个32位字长;对于IPv6数据包,认证数据一定要为整数个64位字长。当认证数据的长度不满足具体要求时,必须添加填充比特,使ICV域的长度达到需要的长度。认证数据的实际长度由所使用的认证算法确定,如采用HMAC-MD5算法时,它的长度为96bits。

2. AH传输模式

如图3-5所示,在传输模式下,AH包头插在IP包头之后,TCP、UDP或者ICMP等上层协议包头之前。一般AH为整个数据包提供完整性检查,但是在传输过程中,某些IP头字段会发生变化,且发送方无法预测数据包到达接收端时此字段的值,例如生存期(Time To Live)或服务类型(Type of Service)等值可变字段(可变字段如图3-6中灰色字段),在进行完整性检查时,应将这些值的可变字段置为0。AH尽可能为IP头和上层协议数据提供足够多的认证,但AH并不能保护可变字段值,因此,AH提供给IP头的保护有些是零碎的。

版本	头长度	服务类型	报文总长度	
标识			标志	分段偏移
生存期		协议号	头校验和	
源IP地址				
目的IP地址				

图3-6 IP头中的可变字段

通常,当用于IPv6时,AH出现在IPv6逐跳路由头之后,IPv6目的选项之前;而用于IPv4时,AH跟随主IPv4头。

3. AH 隧道模式

以上介绍的是传输模式下的 AH 协议，AH 隧道模式与传输模式略有不同。

在隧道模式下，整个原数据包被当做有效载荷封装起来，外面附上新的 IP 包头。其中“内部”IP 包头（原 IP 包头）指定最终的信源和信宿地址，而“外部”IP 包头（新 IP 包头）中包含的常常是做中间处理的网关地址。

与传输模式不同，在隧道模式中，原 IP 地址被当做有效载荷的一部分，受到 IPSec 的保护。另外，通过对数据加密，还可以将数据包目的地址隐藏起来，这样更有助于保护端对端隧道通信中数据的安全性。

图 3-7 给出了 AH 隧道模式中的认证部分。AH 隧道模式为整个数据包提供完整性检查和认证，认证功能优于 ESP。但在隧道技术中，AH 协议很少单独实现，通常与 ESP 协议组合使用。



图 3-7　AH 隧道模式

4. AH 协议对外出数据包的处理流程

AH 协议对外出数据包的处理流程如图 3-8 所示。

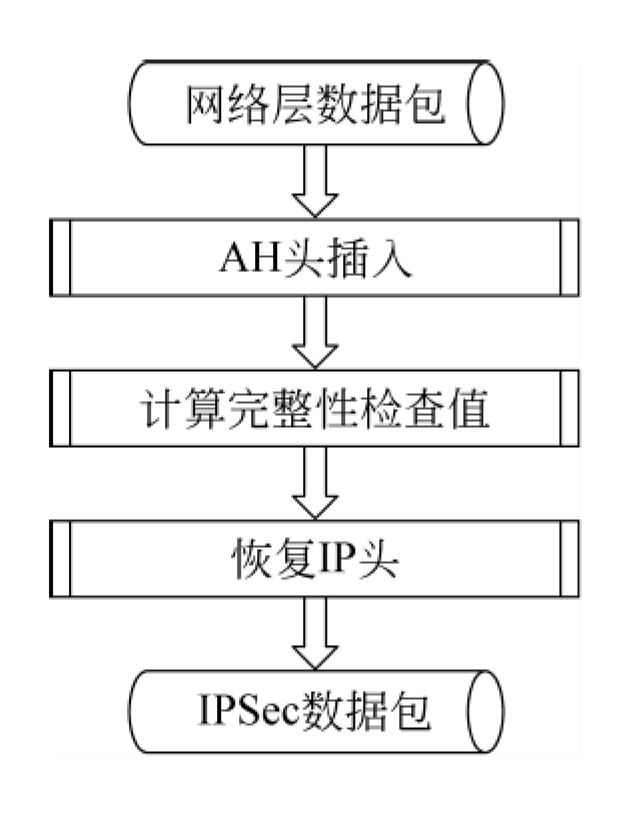


图 3-8　AH 协议对外出数据包的处理流程

AH 协议对外出数据包的处理流程如下。

（1）AH 头插入。在传输模式下，AH 头插在 IP 头之后，各字段的值如下。

① SPI 字段值是来自于处理这个外出数据包 SA 中的 SPI。

② 序列号字段值是当前序列号计数器的值。

③ 下一个头字段值是 TCP 头的协议字段值，该值为 6，表示是 TCP。

对于隧道模式，AH 头插在整个 IP 数据包前面，AH 头的“下一个头”字段值是 4，表示是 IP-in-IP。其他值的计算方法与传输模式相同。

在 AH 头前必须新增一个 IP 头，并填写相应的字段。

① 源地址字段值取自源 AH 设备的 IP 地址。

② 目的 IP 地址字段值从处理该数据包的 SA 中获取。

③ 协议字段值为 51，代表是 ESP。

④ 其他字段值按常规方式填写。

（2）完整性检查值（ICV）计算步骤。

① 在计算 ICV 之前，将 IP 头中可变字段值置为 0，并且 AH 头的认证数据字段也置

为0。这些被置为0的字段不能省略掉，以保证ICV计算结果的对齐性，并且在传输过程中也不会改变这些字段的长度。

② 认证数据字段的填充。有些认证算法可能需要对认证数据字段进行填充，以确保AH头的长度是32位的整数倍。如果认证算法的ICV长度为96位(如MD5或SHA算法)，则不需要填充项。如果认证算法的ICV长度不是32的整数倍，则发送方需要在计算ICV前填充认证数据字段，填充的内容任意。这些填充字节参与ICV的计算，作为计算载荷长度的一部分，并放置在认证数据字段的后面进行传输，以确保接收方正确地执行ICV计算。

③ 隐式填充。有些认证算法要求认证数据长度必须是一个数据块的整数倍。如果IP数据包长度(包括AH)不符合算法的要求，则必须在数据包的末尾进行隐式填充。填充的8位组必须是0，其长度由认证算法确定，隐式填充项不随数据包一起传送。

④ 认证算法计算需要认证的数据，然后将计算结果ICV复制到AH头的"验证数据"字段中。

(3) 恢复IP头。恢复IP头中那些被置为0的字段值。

如果经过AH封装，IP数据包长度大于物理网络的最大帧长，则由IP协议进行统一的分段处理和传输，而AH不做分段检查。

5. AH协议对进入数据包的处理流程

AH协议对进入数据包的处理流程如图3-9所示。

AH协议对进入数据包的处理流程如下。

(1) 数据包组装。由IP协议对分段传输的IP数据包进行组装，然后提交给AH处理。

(2) SA查找。利用三元组<SPI，目的IP地址，AH>在SAD中查找处理这个数据包的SA。如果SA存在，则继续处理，否则丢弃该数据包。

(3) 抗重播检查。检查AH头的序列号字段。如果序列号是有效的，则说明它不是一个重复的数据包，须继续处理；否则丢弃该数据包。

(4) 完整性验证。

① 将AH头认证数据字段中的ICV值保存下来，然后将ICV置为0。

② 将IP头中可变字段置为0。

③ 如果使用的认证算法需要进行隐式填充，则在数据包的末尾执行填充。

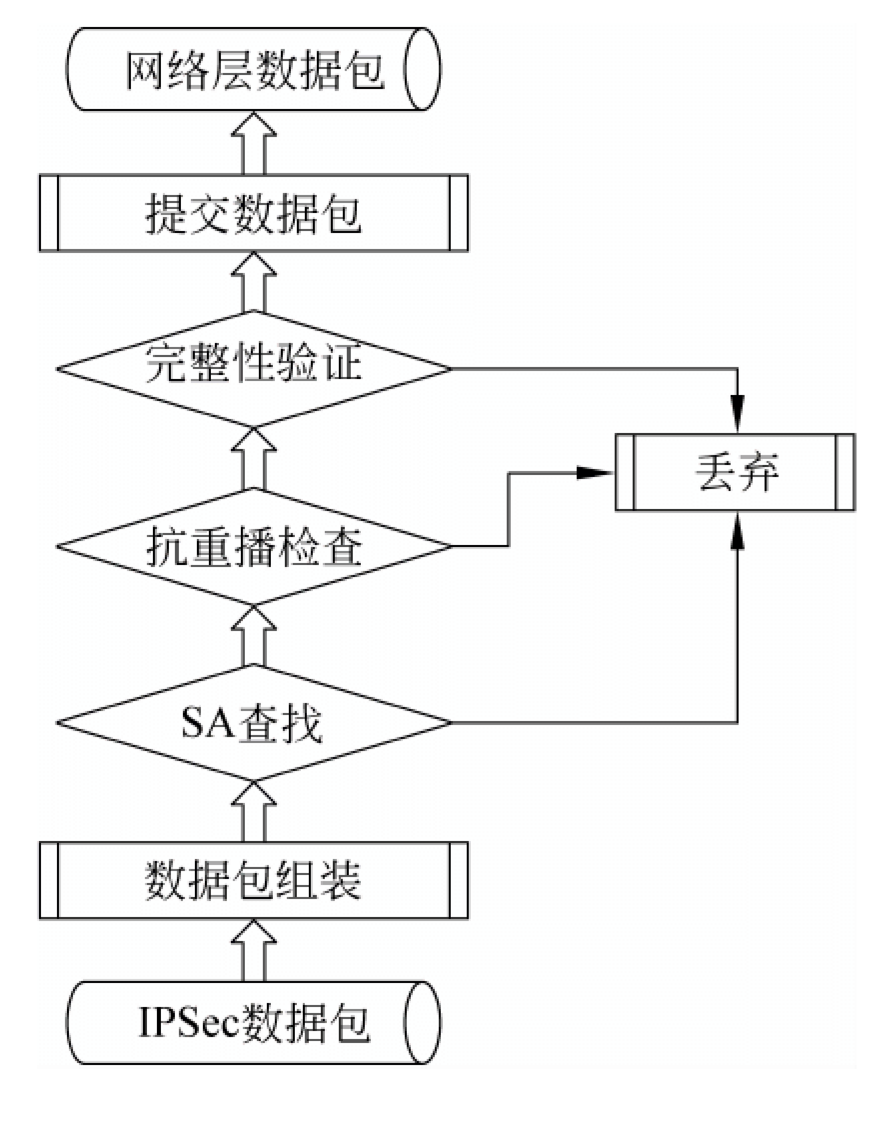


图3-9 AH协议对进入数据包的处理流程

④ 使用相同的认证算法，对需要验证的数据进行计算，计算结果与保存下来的ICV值进行比较。如果匹配，则继续处理，否则丢弃该数据包。

⑤ 提交数据包：对于传输模式，上层协议头和IP头是同步的，只需要将AH头的

“下一个头”字段的值复制到 IP 头的协议字段,并计算出一个新的 IP 校验和。然后将该数据包提交给相应的协议处理。

对于隧道模式,首先去除外部 IP 头和 AH 头,恢复原 IP 数据包。如果该数据包是一个分段,则将得到的该数据包重新插入到 IP 数据流中。

3.3.2 Encapsulating Security Payload 协议

IPSec 封装安全负载(IPSec ESP)是 IPSec 体系结构中的一种主要协议,其主要设计目的是为 IPv4 和 IPv6 中提供安全服务的混合应用。IPSec ESP 通过加密需要保护的数据以及在 IPSec ESP 的数据部分放置这些加密的数据,来提供机密性和完整性。根据用户安全要求,这个机制既可以用于加密一个传输层的段(如 TCP、UDP、ICMP、IGMP),也可以用于加密整个 IP 数据包。封装受保护数据是非常必要的,这样就可以为整个原始数据包提供机密性。

ESP 为 IP 数据包提供完整性检查、认证和加密,可以看做是“超级 AH”,因为它提供机密性并防止篡改。ESP 服务依据建立的关联(SA)是可选的。然而也有如下一些限制。

(1) 完整性检查和认证一起进行。

(2) 仅当与完整性检查和认证一起时,重播(Replay)才是可选的。

(3) “重播”只能由接收方选择。

ESP 的加密服务是可选的,但如果启用加密,也就同时选择了完整性检查和认证。因为如果仅使用加密,入侵者就可能伪造包,以发动密码分析攻击。

ESP 可以单独使用,也可以和 AH 结合使用。一般 ESP 不对整个数据包加密,而是只加密 IP 包的有效载荷部分,不包括 IP 头。但在端对端的隧道通信中,ESP 需要对整个数据包加密。

1. ESP 协议格式

认证包头 AH 协议并不对数据加密,数据对黑客来说仍然清晰可见。当要求对数据保密时,就应使用加密的 ESP(Encapsulating Security Payload)包头。但是,ESP 头中的所有字段都是不加密的。

ESP 提供机密性、数据源认证、无连接的完整性、抗重播服务(一种部分序列完整性的形式)和有限信息流机密性。所提供服务集由安全连接(SA)建立时选择的选项和实施的布置来决定,机密性的选择与所有其他服务相独立。但是,使用机密性服务而不带有完整性/认证服务(在 ESP 或者单独在 AH 中),可能使传输受到某种形式的攻击,以破坏机密性服务。数据源验证和无连接的完整性是相互关联的服务,它们作为一个选项,与机密性(可选择的)结合,提供给用户。只有选择数据源认证时,才可以选择抗重播服务,由接收方单独决定抗重播服务的选择。

如图 3-10 所示,ESP 包头插在 IP 包头之后、TCP 或 UDP 等传输层协议包头之前。

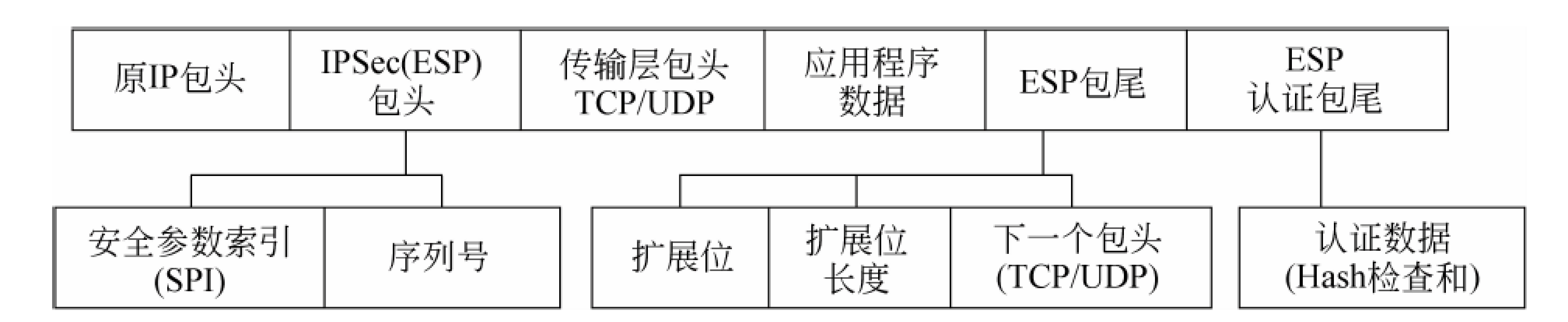


图 3-10　ESP 包头、包尾和认证包尾

ESP 头可以放置在 IP 头之后、上层协议头之前（传输层），或者在被封装的 IP 头之前（隧道模式）。IANA 分配给 ESP 一个协议数值 50，在 ESP 头前的协议头总是在 Next Head 字段（IPv6）或“协议”（IPv4）字段里包含值 50。ESP 包含一个非加密协议头，后面是加密数据。该加密数据既包括了受保护的 ESP 头字段，也包括了受保护的用户数据，这个用户数据可以是整个 IP 数据包，也可以是 IP 的上层协议帧（如 TCP 或 UDP）。

ESP 协议格式如图 3-11 所示。

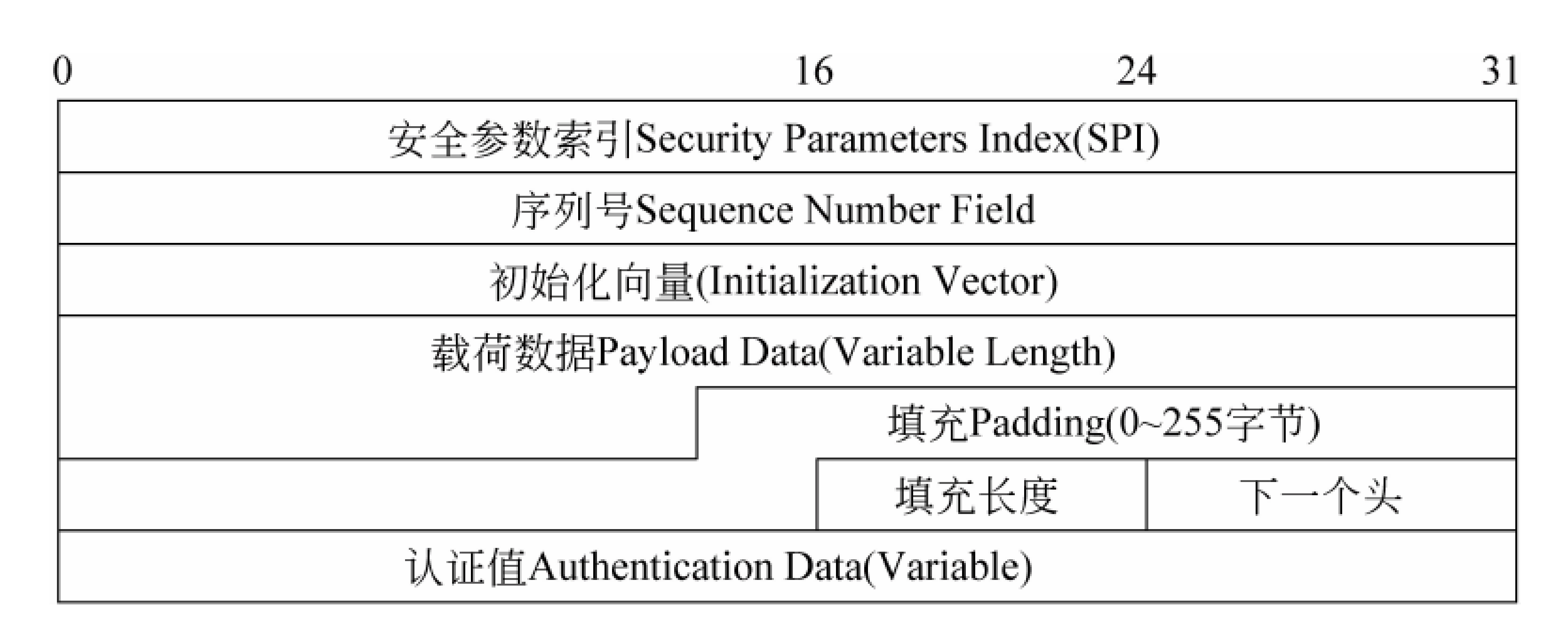


图 3-11　ESP 协议格式

ESP 数据包由 4 个固定长度的域和 3 个变长域组成。具体内容如下。

（1）Security Parameters Index：一个伪随机值，用于识别数据包的安全关联（Security Association，SA）。与 AH 协议一样，接收方可由此确定报文所用的 SA。

（2）Sequence Number Field：从 1 开始的 32 位单增序列号，不允许重复，唯一标识了每一个发送数据包，为关联提供反重播。接收端校验序列号为该字段值的数据包是否已经被接收过，若是，则拒收该数据包。包含无变化的增长计数器值，该值是强制性的，即使接收端不为特定的 SA 提供抗重播服务，它仍然存在。

（3）Initialization Vector：包含于载荷数据字段，用于启动 ESP 的加密过程。是否需要初始化向量，视加密算法而定。

（4）Payload Data：一个可变长字段，包括 Next Header 字段中描述的数据。

（5）Padding：供加密使用。0～255 个字节。DH 算法要求数据长度（以位为单位）对 512 取模后结果为 448，若应用数据长度不足，则用扩展位填充。

（6）Pad Length：接收端根据该字段长度去除数据中扩展位。

（7）Next Header：识别包含在有效负载数据字段中的数据类型。如 IPv6 中的扩展头或上层协议标识符。

(8) Authentication Data：完整性检查和，一个可变长字段，完整性检查部分包括 ESP 包头、有效载荷(应用程序数据)和 ESP 包尾。

ESP 包头中多数字段含义同 AH，如果加密算法要求明文成为密钥长度的整数倍，Padding 字段用于扩展明文到需要的长度。由于 ESP 同时提供了机密性以及身份验证，所以 SA 中必须同时定义两套算法，一是用来确保机密性的算法，叫做加密器 Cipher，二是负责身份验证的算法，叫做验证器 Authenticator，每个 ESP SA 都至少有一个加密器和一个验证器。加密器提供机密性，数据完整性则由身份检验器提供。

2. ESP 传输模式

ESP 协议加密范围如图 3-12 所示。



图 3-12　ESP 的加密部分和完整性检查部分

如图所示，ESP 包头的位置在 IP 包头之后，TCP、UDP 或者 ICMP 等传输层协议包头之前。如果已经有其他 IPSec 协议使用，则 ESP 包头应插在其他任何 IPSec 协议包头之前。ESP 认证包尾的完整性检查部分包括 ESP 包头、传输层协议包头、应用数据和 ESP 包尾，但不包括 IP 包头，因此 ESP 不能保证 IP 包头不被篡改。ESP 加密部分包括上层传输协议信息、数据和 ESP 包尾。

3. ESP 隧道模式

ESP 隧道模式与传输模式略有不同。在隧道模式下，整个原数据包被当做有效载荷封装起来，外面附上新的 IP 包头。其中内部 IP 包头(原 IP 包头)指定最终的信源和信宿地址，而外部 IP 包头(新 IP 包头)中包含的常常是做中间处理的网关地址。

与传输模式不同，在隧道模式中，原 IP 地址被当做有效载荷的一部分，受到 IPSec 保护。另外，通过对数据加密，还可以将数据包目的地址隐藏起来，这样更有助于保护端对端隧道通信中数据的安全性。

ESP 隧道模式中的签名部分(完整性检查和认证部分)和加密部分分别如图 3-13 所示。ESP 的签名不包括新 IP 头。



图 3-13　ESP 隧道模式

4. 外出数据包的处理

ESP 协议对外出数据包的处理流程如图 3-14 所示。

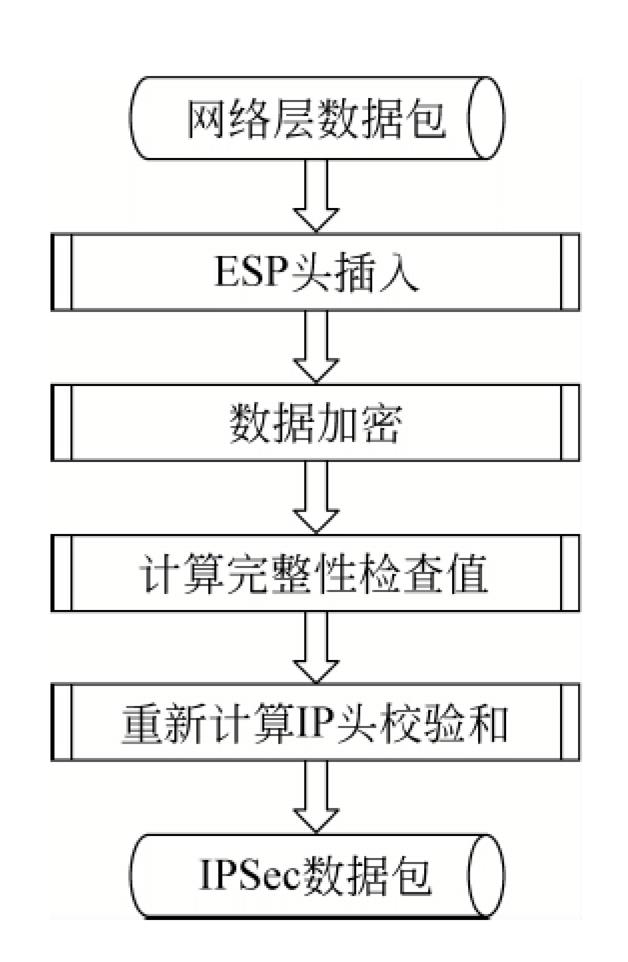


图 3-14 ESP 协议对外出数据包的处理流程

ESP 协议对外出数据包的处理流程如下。

(1) ESP 头插入。在传输模式下,ESP 头插在 IP 头之后。各字段的值如下。

① SPI 字段值来自于处理这个外出数据包 SA 中的 SPI。

② 序列号字段值是当前序列号计数器的值。

③ 填充项字段值是根据密码算法的要求进行填充的。

④ 填充项长度字段值是填充项的长度值。

⑤ 下一个头字段值是 TCP 头的协议字段值,该值为 6,表示是 TCP。

对于隧道模式,ESP 头插在整个 IP 数据包前面,ESP 头的“下一个头”字段值是 4,表示是 IP-in-IP。其他值计算方法与传输模式相同。

在 ESP 头前,必须新增一个 IP 头,并填写相应的字段,内容如下。

① 源地址字段值取自源 ESP 设备的 IP 地址。

② 目的 IP 地址字段值从处理该数据包的 SA 中获取。

③ 协议字段值为 50,代表是 ESP。

④ 其他字段值按常规方式填写。

(2) 数据加密处理步骤如下。

① 从 SA 中得到加密算法和密钥。

② 如果加密算法要求明文的长度是 32 位的整数倍,则进行必要的填充。

③ 如果需要显式的密码同步数据,则将其输入加密算法,并放入载荷数据内;如果需要隐式的密码同步数据,则在本地创建,并输入加密算法。

④ 对数据包进行加密。

(3) 完整性检查值(ICV)计算步骤如下。

① 从 SA 中得到认证算法。

② 如果选择的认证算法要求认证的数据长度必须是 32 位的整数倍,则需要在“下一个头”字段后执行隐式填充。填充的 8 位组必须是 0,其长度由认证算法确定。所谓隐式填充,是指它不随数据包一起传送。

③ 认证算法计算需要认证的数据,然后将计算结果 ICV 复制到“验证数据”字段中。

(4) 重新计算 IP 头校验和。重新计算新 IP 头中的校验和字段值。

如果经过 ESP 封装的 IP 数据包长度大于物理网络的最大帧长,则由 IP 协议进行统一的分段处理和传输,而 ESP 不做分段检查。

5. 进入数据包的处理

ESP 协议对进入数据包的处理流程如图 3-15 所示。

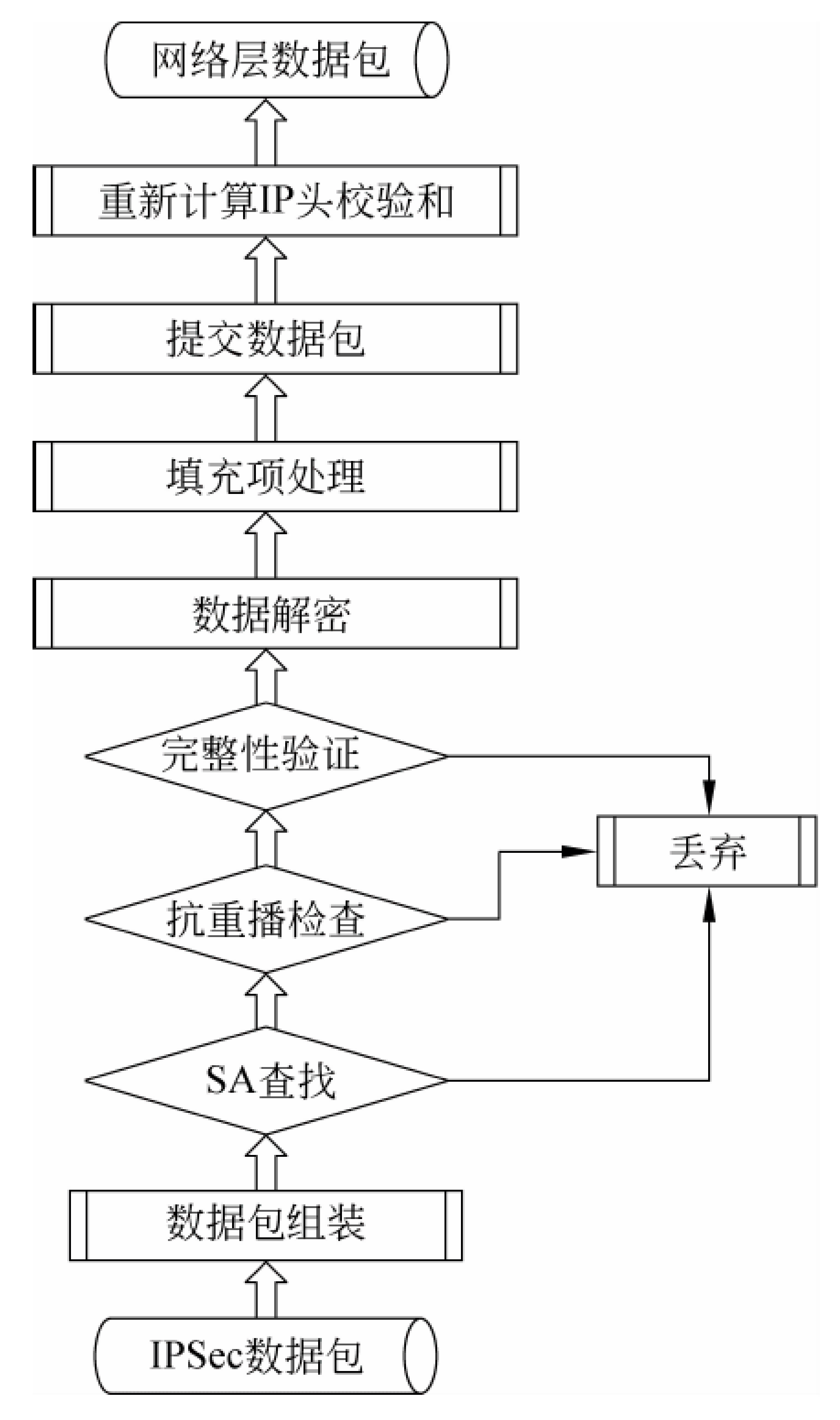


图 3-15 ESP 协议对进入数据包的处理流程

(1) 数据包组装。由 IP 协议对分段传输的 IP 数据包进行组装，然后提交给 ESP 处理。

(2) SA 查找。利用三元组<SPI，目的 IP 地址，ESP>在 SAD 中查找处理这个数据包的 SA。如果 SA 存在，则继续处理，否则丢弃该数据包。

(3) 抗重播检查。检查 ESP 头的序列号字段。如果序列号是有效的，则说明它不是一个重复的数据包，须继续处理；否则丢弃该数据包。

(4) 完整性验证。首先提取和保存 ESP 中认证数据字段值，然后使用相同的认证算法，对需要验证的数据进行计算，计算结果与保存下来的认证字段值进行比较。如果匹配，则继续处理，否则丢弃该数据包。

(5) 数据解密步骤如下。

① 通过 SA 获取解密算法和密钥。

② 如果指定了显式的密码同步数据，则从载荷中获取该数据，并输入解密算法；如果指定了隐式的密码同步数据，则由本地创建密码同步数据，然后输入解密算法。

③ 对 ESP 数据包进行解密。

(6) 填充项处理步骤如下。

① 检查正确性。如果填充项是由加密算法指定的，则检查是否符合算法所要求的格式；如果填充项是通过默认填充方案生成的，则检查其是否是从 1 开始单向递增的。

② 将填充项从载荷中去除。

(7) 提交数据包。对于传输模式，上层协议头和 IP 头是同步的，只需要将 ESP 头的“下一个头”字段的值复制到 IP 头的协议字段，并计算出一个新的 IP 校验和。然后将该数据包提交给相应的协议处理。

对于隧道模式，首先去除外部 IP 头和 ESP 头，恢复原 IP 数据包。如果该数据包是一个分段，则将该数据包重新插入到 IP 数据流中。

3.3.3 安全协议适用范围

如图 3-16 所示，主机 A 有一个私有 IP 地址，这些地址在公网上是不被路由的。为了

让使用这些地址的主机和位于它们所在网络之外的主机进行通信，以这些外部主机为目的地的数据流在离开源网络之前，需要经过一个网络地址转换(NAT)网关。NAT 网关将流出的数据包的源地址域的私有 IP 地址替换为指定的公网 IP 地址，重新计算校验和，并将数据包转发给指定的目的地址。

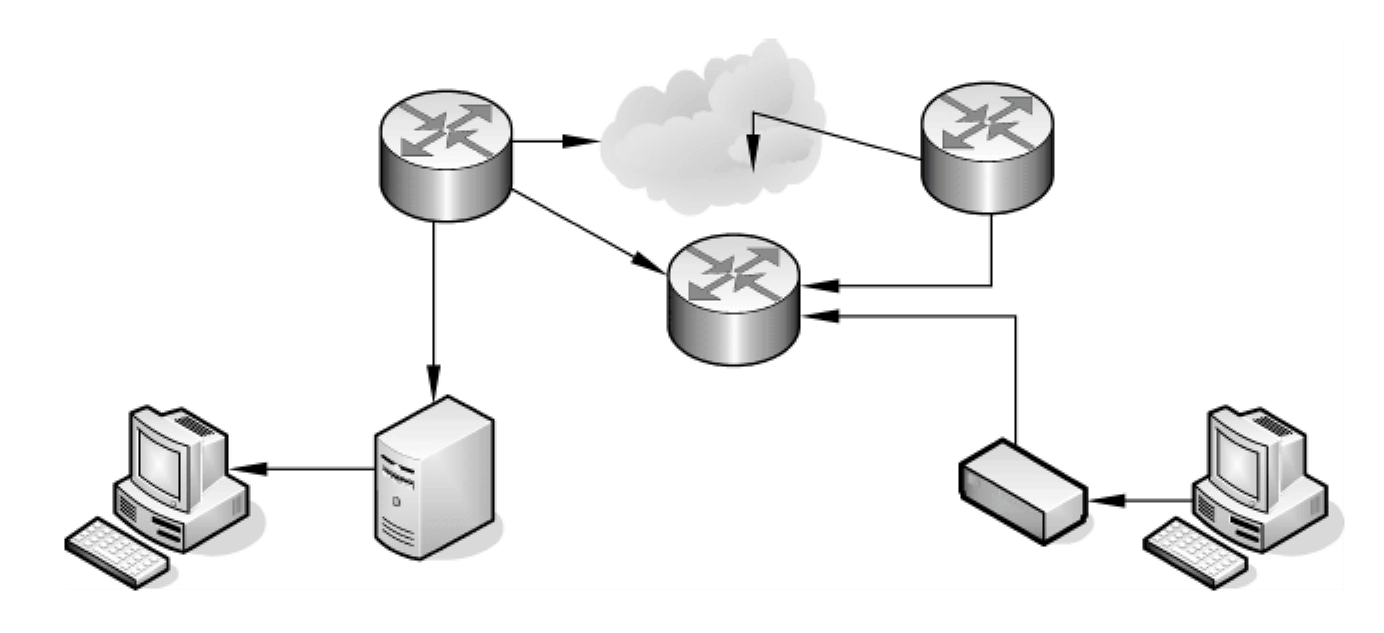


图 3-16　AH 协议不适用情况

如果主机 A 和主机 B 的 AH 认证均被启用，当数据包到达主机 B，AH 完整性校验将失败。主机 B 计算出来的完整性校验值将和主机 A 计算出来的不同，因为 NAT 网关修改了数据包的源地址域。

3.4　安全关联

3.4.1　安全关联(SA)

安全关联(SA)是通信对等方之间对某些要素的一种协定，如对保护的通信数据需要的加密算法、验证算法、密钥、生存时间等。安全关联是单工的(即单向的)，对于保护常见的双向通信来说，每个方向上都需要建立一个安全关联。因此，输入和输出的数据流需要独立的 SA，如图 3-17 所示。

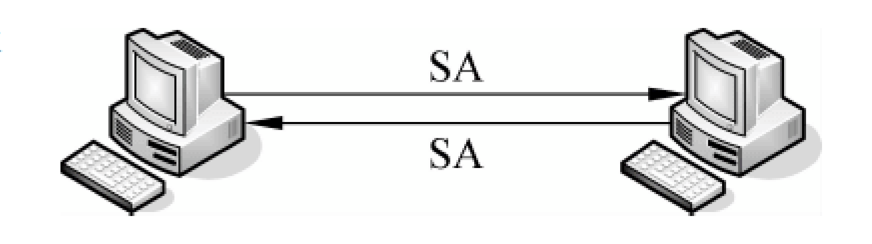


图 3-17　SA 的单向特性

一个安全关联使用 AH 协议或 ESP 协议，但二者不同时使用在一个安全关联上。如果需要由 AH 协议和 ESP 协议同时为一条通信流提供安全服务，就要建立两个或两个以上的安全关联来保护这一通信流。在多个 SA 的情况下，必须将一个 SA 序列组合成 SA 束，经过 SA 束处理后的通信能够满足一个安全策略。SA 束中的 SA 顺序是由安全策略定义的，各个 SA 可以终止于不同的端点，将多个 SA 组合成 SA 束的方法有以下两种。

1. 传输邻接

将 AH 和 ESP 的传输模式组合起来保护一个 IP 数据包，具体形式如图 3-18 所示。通常这种方法只允许一层组合，因为每个协议只要使用足够健壮的密码算法，安全性是有保证的，并不需要多层嵌套使用，以减少协议的处理开销。

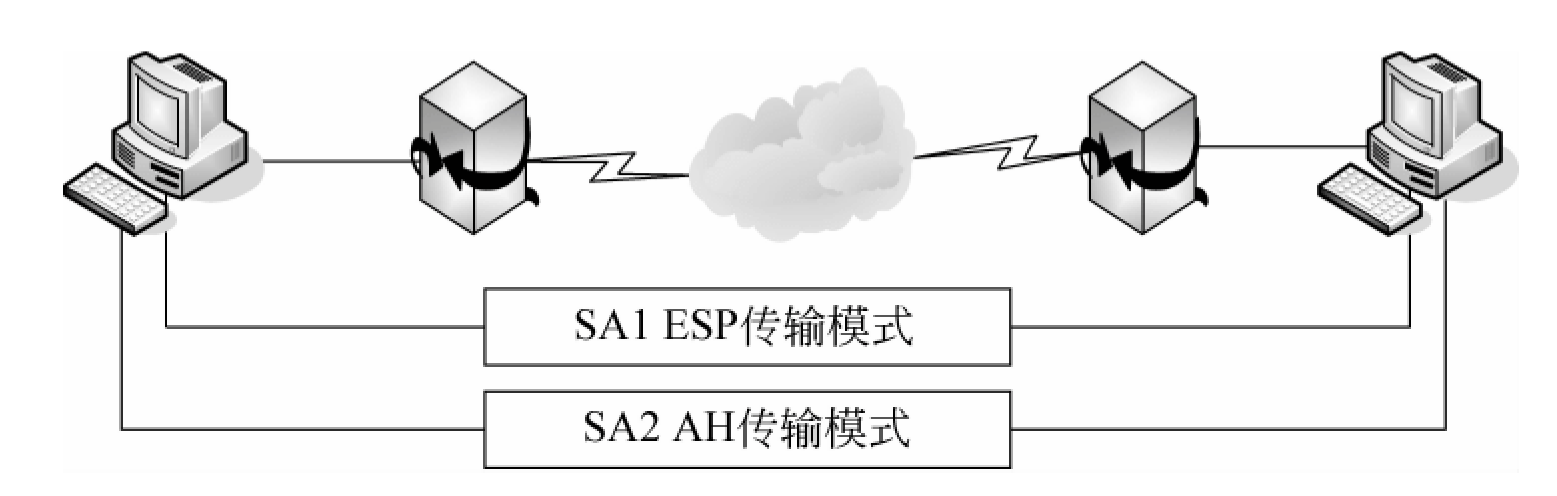


图 3-18　传输邻接模式

2. 多重隧道

这种方法由多个 SA 组合成一个多重隧道，保护 IP 数据包。每个隧道都可以在不同的 IPSec 结点上开始或终止。多重隧道可以分成如下 3 种形式。

(1) 由两个多 SA 端点组合而成。由两个多 SA 端点组合而成的传输模式如图 3-19 所示。

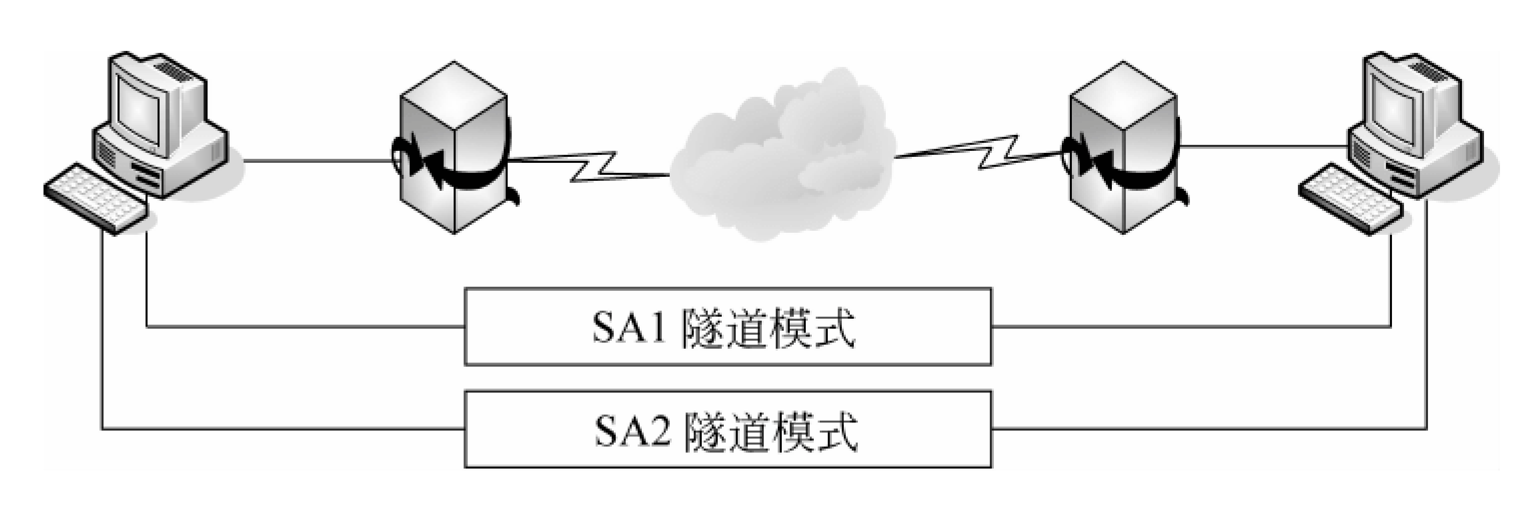


图 3-19　多重隧道模式一

(2) 由一个多 SA 端点和一个单 SA 端点组合而成。由一个多 SA 端点和一个单 SA 端点组合而成的传输模式如图 3-20 所示。

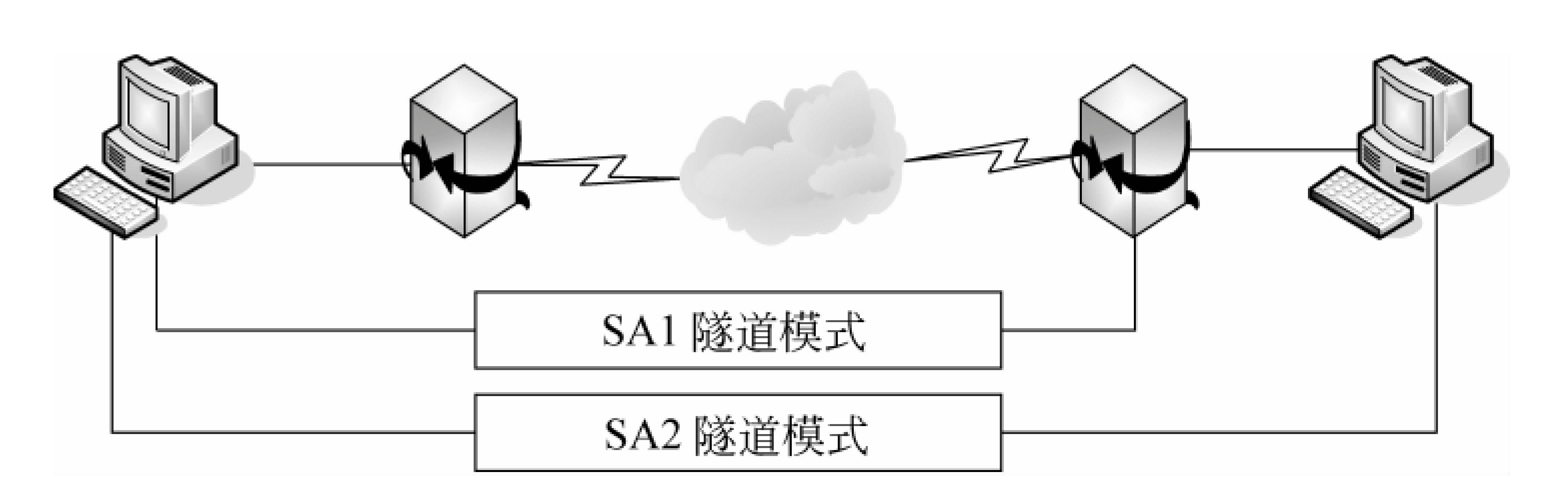


图 3-20　多重隧道模式二

(3) 由多个单 SA 端点组成。由多个单 SA 端点组成的传输模式如图 3-21 所示。

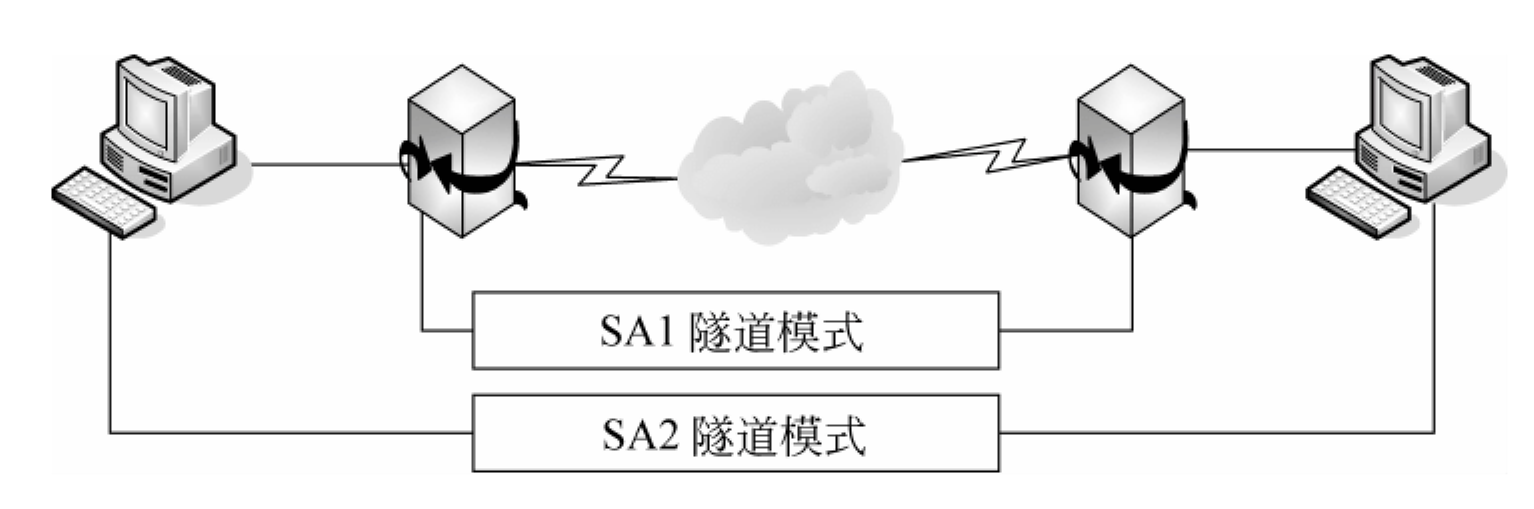


图 3-21　多重隧道模式三

另外,传输模式和隧道模式还可以组合使用。例如,用一个隧道模式的 SA 和一个传输模式的 SA,按顺序组合成一个 SA 束。对于安全协议的使用顺序,在传输模式下,如果 AH 和 ESP 组合使用,则 AH 应当位于 ESP 之前,AH 作用于 ESP 生成的密文;在隧道模式下,可以按照不同的顺序使用 AH 和 ESP。

3.4.2 安全关联模型

IPSec 处理 IP 报文的具体细节取决于 IPSec 协议的具体实现,IPSec 协议没有对此作出规定。但是,为了满足互操作性,并且具有最基本的管理能力,协议处理的外在特性必须有统一的要求。因此,IPSec 协议规范给出了一个外在特性的模板,该模板包含安全策略数据库(Security Policy Database,SPD)、安全关联数据库(Security Association Database,SAD)和选择器。SPD 存放对于出入一个主机或安全网关的 IP 报文所应采取的安全策略;SAD 存放系统所有的安全关联和它们所使用的参数。安全策略是网络安全系统的重要组成部分和灵魂,安全关联就是它的最终体现和执行形式。二者有机结合,缺一不可。

1. 安全策略数据库 SPD

SPD 指明了以什么方式为 IP 数据包提供安全服务,是 SA 处理的重要元素之一,它定义了安全策略相关参数的存储和管理结构。

对于所有的 IP 通信,不论它是进入的还是外出的,都必须通过 SPD。因此,SPD 必须为进入的和外出的 IP 通信提供不同的入口,可以把它们看成是形式上分离的 SPD。

一个 SPD 必须能区分两种情况,即被实施了 IPSec 处理的通信和无须实施 IPSec 处理的通信。

对于任何进入和外出的 IP 数据包,都有如下 3 种处理选择。

(1) 丢弃处理。不允许一个数据包离开主机、通过安全网关或提交给一个应用。

(2) 旁路 IPSec 处理。允许一个数据包在不经过任何 IPSec 保护的情况下通过。

(3) 实施 IPSec 处理。对一个数据包实施了 IPSec 处理。在这种情况下,SPD 必须指明所需提供的安全服务以及所采用的协议和算法等。

一个安全策略实例如表 3-1 所示。

表 3-1 一个安全策略实例

SA 描述	选择器		标识
A	166.168.2.7	…	丢弃
B	166.168.2.8	…	旁路
C	192.168.2.0/24	…	实施 IPSec 处理
D	166.168.2.3	…	实施 IPSec 处理
E	192.168.2.1	…	实施 IPSec 处理
…	…	…	…

如果 SPD 策略条目允许的源地址是通配符形式，则 SPD 条目中选择器的值也是通配符形式。

由于选择器的值可以是通配符，因此两个策略条目的匹配范围可能会重叠。为了保证一致的、可预测的处理，SPD 条目必须经过排序，且总是以相同的顺序对条目进行查找，从而使第一个匹配的条目总是被首先选中。

2. 安全联盟数据库(SAD)

SAD 是一种形式上的数据库，每个 SA 都对应于 SAD 中的一个条目，定义了一个与 SA 相关的参数。如 AH/ESP 算法和密钥、顺序号、协议模式以及生命周期等。

对于外出数据包的处理，SA 是由 SPD 中的条目指示的，即由 SPD 来确定所使用的 SA。当一个 SPD 条目没有指向一个特定的 SA 时，IPSec 系统则创建一个相关的 SA 或者 SA 束，并且与一个 SPD 条目或 SAD 条目相关联。

对于进入数据包的处理，每个 SAD 中条目通过一个三元组＜目的 IP 地址；IPSec 协议类型；SPI＞来索引和查找，以确定对进入数据包进行处理的 SA 或 SA 束。

目的 IP 地址：外部 IP 头中的目的 IP 地址。

IPSec 协议类型：AH 或 ESP。

SPI：用于区分目的 IP 地址相同且 IPSec 协议类型相同的 SA。

3. 选择器

选择器是用来定位安全策略数据库中的一个策略。一个 SA 或 SA 束可以是细粒度的，也可以是粗粒度的，取决于为 SA 定义通信集时所使用的选择器。

例如，两个主机之间所有的通信可以由一个单独的 SA 处理，并且提供了一个统一的安全服务集合。同样，两个主机之间所有的通信也可以由多个 SA 处理，并且不同的 SA 提供不同的安全服务。

使用 SAD、SPD 和选择器对进入数据包和外出数据包处理时的流程分别如图 3-22 和图 3-23 所示。

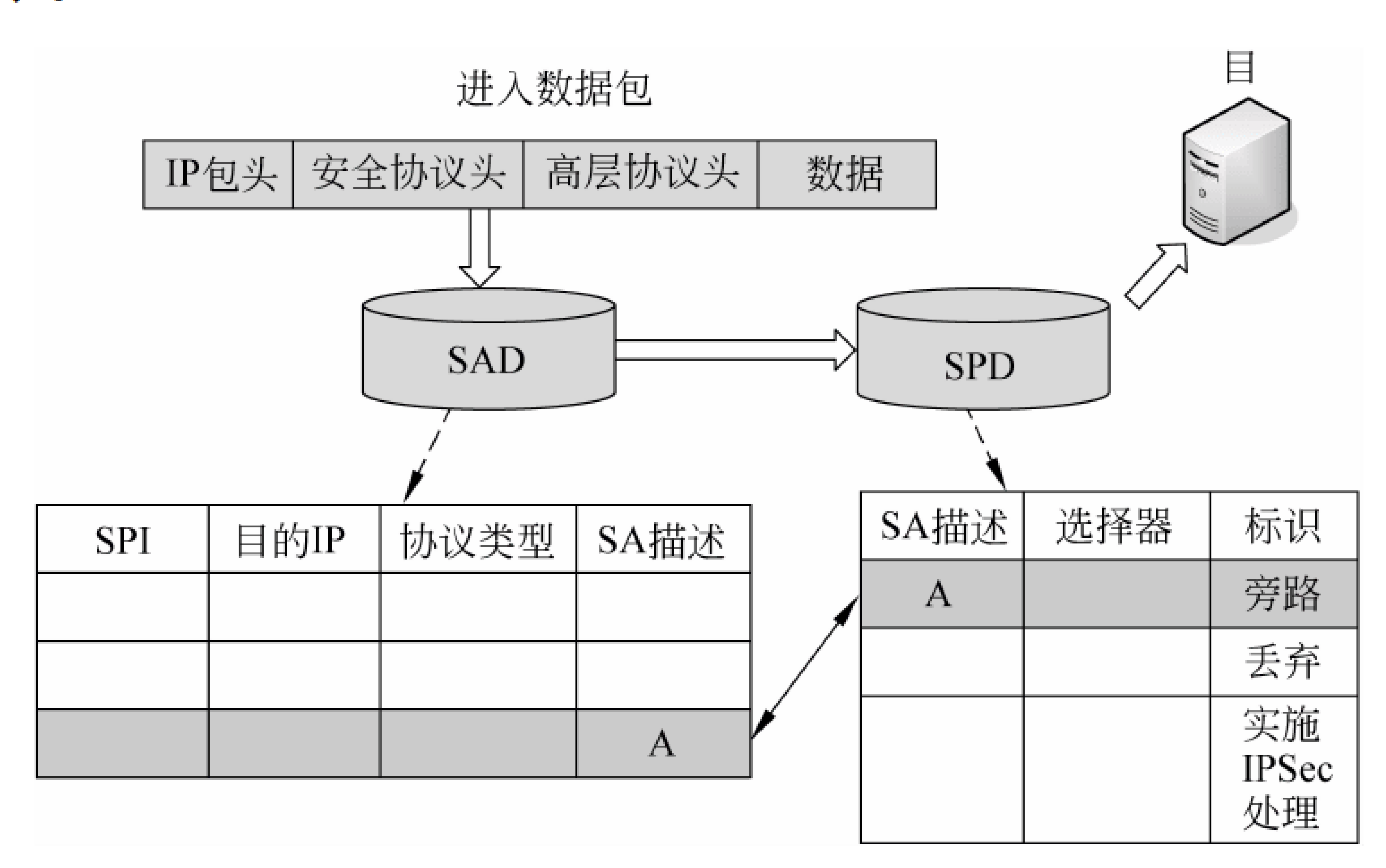


图 3-22　对于进入数据包的处理

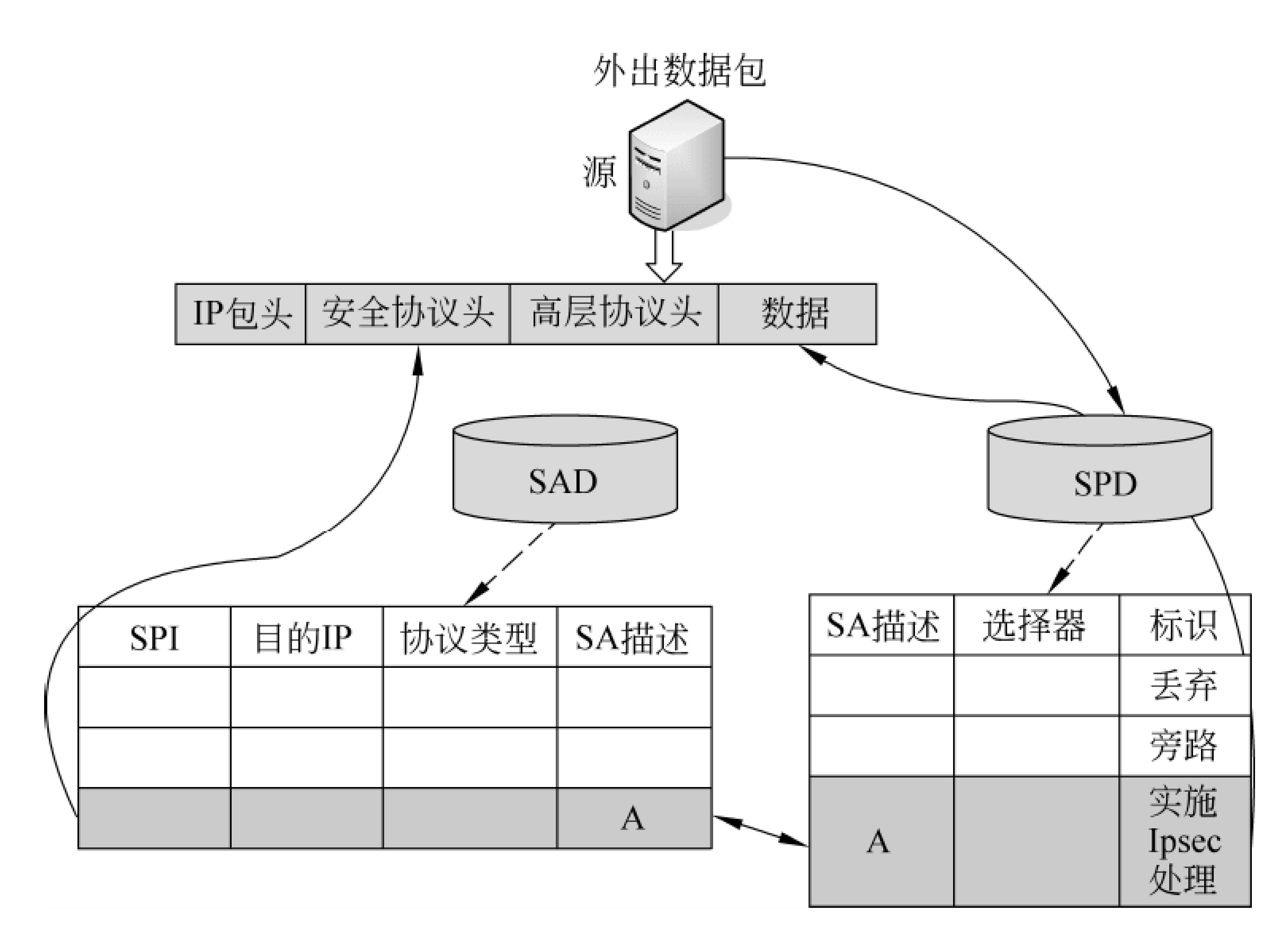


图 3-23 对于外出数据包的处理

3.5 IPSec 密钥交换机制

在使用 IPSec 保护一个 IP 数据包之前，必须先建立一个 SA，SA 可以手工创建，也可以自动创建。自动建立 SA 时，要使用 IKE 协议。IKE 代表 IPSec 进行 SA 的协商，并将协商好的 SA 填入 SAD 中。

3.5.1 Internet 密钥交换

1. IKE 技术

IKE 的作用是在 IPSec 通信双方之间建立起共享安全参数以及检验过的密钥，即动态建立安全关联 SA。由 RFC 2409 文档描述的 IKE 是一个建立在三种协议（ISAKMP、Oakley、SKEME）之上的混合协议，沿用了 ISAKMP（Internet 安全关联和密钥管理协议）的框架基础、Oakley 的模式、SKEME 的共享和密钥更新技术，从而定义出自己的验证加密材料生成技术以及协商共享策略。

ISAKMP 是 Internet 安全关联和密钥管理协议，为认证和密钥交换提供一个框架，但没有对它们进行具体定义。ISAKMP 被设计为独立于密钥交换协议，即它可以支持多种不同的密钥交换协议。ISAKMP 是一个应用层协议，它不仅可管理 IPSec 协议所辖的安全关联和密钥，而且也适用于其他网络安全协议（如传输层安全协议）。ISAKMP 定义了双方如何沟通，如何构建彼此沟通的信息，还定义了保障通信安全所需要的状态变换。ISAKMP 提供了对双方身份进行验证的方法，密钥交换时交换信息的方法，以及对安全服务进行协商的方法。

Oakley 描述了一系列密钥交换模式，以及每种模式所提供服务的细节（如密钥的身

份保护、认证)。

SKEME 描述了一种通用的密钥交换技术,这种技术提供了基于公共密钥的身份认证和快速密钥刷新,定义了通信双方建立一个共享验证密钥所必须采取的步骤。

ISAKMP 只对认证和密钥交换提出了结构框架,但没有具体定义。ISAKMP 与密钥交换相独立,支持多种不同的密钥交换。IKE 是一系列密钥交换中的一种,称为"模式"。

IKE 可用于协商虚拟专用网(VPN),也可用于远程用户(其 IP 地址不需要事先知道)访问安全主机或网络,支持客户端协商。客户端模式即为协商方不是安全连接发起的终端点。当使用客户模式时,端点处的身份是隐藏的。

IKE 的实施必须支持以下的属性值。

(1) DES 用在 CBC 模式,使用弱、半弱、密钥检查。

(2) MD5[MD5]和 SHA[SHA]。

(3) 通过预共享密钥进行认证。

(4) 默认的组 1 上的 MODP。

另外,IKE 的实现也支持 3DES 加密;用 Tiger [TIGER] 作为 Hash;数字签名标准,RSA[RSA],使用 RSA 公共密钥加密的签名和认证;以及使用组 2 进行 MODP。IKE 实现可以支持其他的加密算法,并且可以支持 ECP 和 EC2N 组。只要实现了 IETF IPSec DOI,IKE 模式就必须实施。其他 DOI 也可使用这里描述的模式。

IKE 建立 SA 分两个阶段。第一阶段,协商创建一个通信信道(IKE SA),并对该信道进行认证,为双方进一步的 IKE 通信提供机密性、数据完整性以及数据源认证服务;第二阶段,使用已建立的 IKE SA 建立 IPSec SA。分两个阶段完成这些服务,有助于提高密钥交换的速度。

第一阶段 SA(主模式 SA,为建立信道而进行的安全关联)。第一阶段协商(主模式协商)步骤如下。

(1) 策略协商。这一步就以下 4 个强制性参数值进行协商。

① 加密算法:选择 DES 或 3DES。

② Hash 算法:选择 MD5 或 SHA。

③ 认证方法:选择证书认证、预置共享密钥认证或 Kerberos v5 认证。

④ Diffie-Hellman 组的选择。

(2) DH 交换。虽然名为"密钥交换",但事实上,在任何时候,两台通信主机之间都不会交换真正的密钥,而只是交换一些 DH 算法生成共享密钥所需要的基本材料信息。DH 交换可以是公开的。在彼此交换过密钥生成"材料"后,两端主机可以各自生成完全一样的共享"主密钥",保护紧接其后的认证过程。

(3) 认证 DH 交换需要得到进一步认证。如果认证不成功,通信将无法继续下去。"主密钥"结合第(1)步中确定的协商算法,对通信实体和通信信道进行认证。在这一步中,整个待认证的实体载荷,包括实体类型、端口号和协议,均由前一步生成的"主密钥"提供机密性和完整性保证。

第二阶段 SA(快速模式 SA,为数据传输而建立的安全关联)。这一阶段协商建立 IPSec SA,为数据交换提供 IPSec 服务。第二阶段协商消息接收第一阶段 SA,任何没有

第一阶段SA保护的消息将被拒收。第二阶段协商(快速模式协商)步骤如下。

(1) 策略协商,双方交换需求如下。

① 使用哪种IPSec协议:AH或ESP。

② 使用哪种Hash算法:MD5或SHA。

③ 是否要求加密,若是,选择加密算法:3DES或DES在上述3个方面达成一致后,将建立起两个SA,分别用于入站和出站通信。

(2) 会话密钥"材料"刷新或交换。

这一步将生成加密IP数据包的"会话密钥"。生成"会话密钥"所使用的"材料"可以和生成第一阶段SA中"主密钥"的相同,也可以不同。如果不作特殊要求,只需要刷新"材料"后生成新密钥即可。若要求使用不同的"材料",则在密钥生成之前,首先进行第二轮的DH交换。

(3) SA和密钥连同SPI,递交给IPSec驱动程序。

第二阶段协商过程与第一阶段协商过程类似,不同之处在于,在第二阶段中,如果响应超时,则自动尝试重新进行第一阶段SA协商。

第一阶段SA建立起安全通信信道,保存在高速缓存中,在此基础上,可以建立多个第二阶段SA协商,从而提高整个建立SA过程的速度。只要第一阶段SA不超时,就不必重复第一阶段的协商和认证。允许建立的第二阶段SA的个数由IPSec策略属性决定。

2. SA生命期

第一阶段SA有一个默认有效时间。如果SA超时,或"主密钥"和"会话密钥"中任何一个生命期时间到,都要向对方发送第一阶段SA删除消息,通知对方第一阶段SA已经过期,之后需要重新进行SA协商。

第二阶段SA的有效时间由IPSec驱动程序决定。

3. 密钥生命期

生命期设置决定何时生成新密钥。在一定的时间间隔内,重新生成新密钥的过程称为"动态密钥更新"或"密钥重新生成"。密钥生命期设置决定了在特定的时间间隔之后,将强制生成新密钥。例如,假设一次通信需要10ks,而我们设定密钥生命期为1ks,则在整个数据传输期间,将生成10个密钥。在一次通信中,使用多个密钥保证了即使攻击者截取了单个通信密钥,也不会危及全部通信安全。密钥生命期有一个默认值,但"主密钥"和"会话密钥"生命期都可以通过配置修改。无论是哪种密钥生命期时间到,都要重新进行SA协商。单个密钥所能处理的最大长度不允许超过100Mb。

4. 会话密钥更新限制

反复地从同一个"主密钥"生成材料去生成新的"会话密钥",很可能会造成密钥泄密。"会话密钥更新限制"功能可以有效地限制泄密的可能性。例如,两台主机建立安全关联后,A先向B发送某条消息,间隔数分钟后,再向B发送另一条消息。由于新的SA刚建

立不久，因此两条消息所用的加密密钥很可能是用同一“材料”生成的。如果想限制某密钥“材料”重用次数，可以设定“会话密钥更新限制”。譬如，设定“会话密钥更新限制”为5，意味着同一“材料”最多只能生成5个“会话密钥”。

若启用“主密钥精确转发保密(PFS)”，则“会话密钥更新限制”将被忽略，因为PFS每次都强制使用新“材料”重新生成密钥。将“会话密钥更新限制”设定为1和启用PFS效果是一样的。如果既设定了“主密钥”生命期，又设定了“会话密钥更新限制”，那么无论哪个限制条件先满足，都引发新一轮SA协商。在默认情况下，IPSec不设定“会话密钥更新限制”。

5. Diffie-Hellman(DH)组

DH组决定DH交换中密钥生成“材料”的长度。密钥的牢固性部分决定于DH组的强度。IKE共定义了5个DH组，组1(低)定义的密钥“材料”长度为768位；组2(中)长度为1024位。密钥“材料”长度越长，所生成的密钥安全度也就越高，越难被破译。

DH组的选择很重要。因为DH组只在第一阶段的SA协商中确定，第二阶段的协商不再重新选择DH组。两个阶段使用的是同一个DH组，因此该DH组的选择将影响所有“会话密钥”的生成。

在协商过程中，对等的实体间应选择同一个DH组，即密钥“材料”长度应该相等。若DH组不匹配，将视为协商失败。

6. 精确转发保密(Perfect Forward Secrecy，PFS)

与密钥生命期不同，PFS决定新密钥的生成方式，而不是新密钥的生成时间。PFS保证无论在哪一阶段，一个密钥只能使用一次，而且生成密钥的“材料”也只能使用一次。某个“材料”生成了一个密钥后即被弃，绝不用来再生成任何其他密钥。这样可以确保一旦单个密钥泄密，最多只可能影响用该密钥加密的数据，而不会危及整个通信。

PFS分主密钥PFS和会话密钥PFS。启用主密钥PFS，IKE必须对通信实体进行重新认证，即一个IKE SA只能创建一个IPSec SA。对每一次第二阶段SA的协商，主密钥PFS都要求新的第一阶段协商，这将会带来额外的系统开销。因此使用它要格外小心。

然而，启用会话密钥PFS，可以不必重新认证，因此对系统资源要求较小。会话密钥PFS只要求为新密钥生成进行新的DH交换，即需要发送4个额外消息，但无须重新认证。PFS不属于协商属性，不要求通信双方同时开启PFS。主密钥PFS和会话密钥PFS均可以各自独立设置。

3.5.2 密钥管理协议

Internet安全关联和密钥管理协议(ISAKMP)是IPSec体系结构中的一种主要协议。该协议结合认证、密钥管理和安全连接等概念来建立政府、商家和因特网上的私有通信所需要的安全。

ISAKMP 定义了程序和信息包格式来建立、协商、修改和删除安全管理(SA)。SA 包括了各种网络安全服务执行所需的所有信息,这些安全服务包括 IP 层服务(如头认证和负载封装)、传输或应用层服务,以及协商流量的自我保护服务等。ISAKMP 定义包括交换密钥生成和认证数据的有效载荷,这些格式为传输密钥和认证数据提供了统一框架,而它们与密钥产生技术、加密算法和认证机制相独立。

ISAKMP 区别于密钥交换协议,是为了把安全连接管理的细节从密钥交换的细节中彻底分离出来。不同的密钥交换协议中的安全属性也是不同的。然而,需要一个通用的框架支持 SA 属性格式、谈判、修改与删除 SA,ISAKMP 即可作为这种框架。

ISAKMP 支持在所有网络层安全协议(如 IPSEC、TLS、TLSP、OSPF 等)的 SA 协商。ISAKMP 通过集中管理 SA,减少了在每个安全协议中重复功能的数量。ISAKMP 还能通过一次对整个栈协议的协商来减少建立连接的时间。

1. 消息格式

(1) 头格式。ISAKMP 的消息格式如图 3-24 所示。

8	12	16	24	32 bit
Initiator Cookie				
Responder Cookie				
Next Payload	MjVer	MnVer	Exchange Type	Flags
Message ID				
Length				

图 3-24　ISAKMP 的消息格式

Initiator Cookie: Initiator Cookie(发起者的 Cookie)用于启动 SA 建立、SA 通知或 SA 删除的实体 Cookie。

Responder Cookie: Responder Cookie(响应者的 Cookie)用于响应 SA 建立、SA 通知或 SA 删除的实体 Cookie。

Next Payload: 下一载荷,指示 ISAKMP 消息头之后下一个载荷的类型。ISAKMP 消息载荷的类型如表 3-2 所示,具体载荷的格式和处理参见 RFC 2408。

表 3-2　ISAKMP 消息载荷的类型

值	载荷类型	描　　述
0	NONE	空载荷
1	Security Association(SA)	安全关联载荷(协商安全属性,指示 DOI)
2	Proposal(P)	建议载荷(SA 协商安全机制、变换的建议)
3	Transform(T)	转码载荷(SA 协商特定机制、变换的信息)
4	Key Exchange(KE)	密钥交换载荷(不同的密钥交换技术)

续表

值	载荷类型	描　述
5	Identification(ID)	标识载荷(用于交换载荷的特定 DOI 数据)
6	Certificate(CERT)	证书载荷(传输证书及相关信息)
7	Certificate Request(CR)	证书请求载荷(通过 ISAKMP 请求证书)
8	Hash(HASH)	散列载荷(SA 建立交换期间的哈希结果数据)
9	Signature(SIG)	签名载荷(SA 建立交换期间的数字签名数据)
10	Nonce(NONCE)	Nonce 载荷(保证存活、防重放攻击的随机数)
11	Notification(N)	通知载荷(向对端发送信息数据,如报错)
12	Delete(D)	删除载荷(发送者从 SAD 中删除 SA 的标识符)
13	Vendor ID(VID)	提供商 ID 载荷(厂商定义,标识厂商的实现)
14～127	RESERVED	预留
128～255	Private USE	私有载荷(与载荷 13 搭配使用)

Major Version：使用的 ISAKMP 协议的主版本号。所有 ISAKMP 实现只允许接收低于自身主版本号的消息。

Minor Version：使用的 ISAKMP 协议的副版本号。如果主版本号相同,所有 ISAKMP 实现只允许接收低于自身副版本号的消息。

Exchange Type：正在使用的交换类型。该字段指示了 ISAKMP 交换消息和载荷的顺序。ISAKMP 消息交换的类型如表 3-3 所示。

表 3-3　ISAKMP 消息交换的类型

值	交换类型	描　述
0	NONE	空
1	Base	交换密钥,不进行身份验证
2	Identity Protection	交换密钥,也进行身份验证
3	Authentication Only	只有认证的交换
4	Aggressive	主动交换,类似于 Base 交换
5	Informational	传输信息,用于 SA 管理
6～31	ISAKMP Future Use	未来预留
32～239	DOI Specific Use	DOI 专用
240～255	Private Use	私有专用

Flags：为 ISAKMP 交换设置的各种选项。其中 E(加密位)标志位决定 ISAKMP 的载荷是否进行加密;C(承诺位)标志位用于指示密钥交换的同步;A(认证位)标志位指示

ISAKMP 信息交换携带通知载荷，并对信息传送使用完整性检查的认证算法，但不使用加密算法。

Message ID：唯一的信息标识符，用来识别第二阶段的协议状态。该标识符由发起者在阶段 2 协商中随机生成，在阶段 1 协商期间必须设置为零。

Length：全部信息(头＋有效载荷)长(八位)。

(2) 载荷。ISAKMP 定义了多种不同的载荷，它们都是以相同的头格式开始的，这个通用的头格式如图 3-25 所示。



图 3-25　通用的头格式

① 下一个载荷：跟随在当前载荷之后的 ISAKMP 载荷的类型。

② 保留字段：目前未使用，必须设置为 0。

③ 载荷长度：当前载荷的长度。

ISAKMP 定义的载荷类型如表 3-4 所示。

表 3-4　ISAKMP 定义的载荷

下一个载荷类型	分配的值	下一个载荷类型	分配的值
无	0	证书	6
安全联盟	1	证书请求	7
建议	2	散列	8
转码	3	签名	9
密钥交换	4	Nonce	10
标识	5		

(3) 属性表示。每个转码载荷都包含了一系列属性，它们是这种转码所特有的。这些属性非常灵活，也比较复杂。在 ISAKMP 中，属性是用“类型/值”对的形式表现的。每种属性都由其类型指定，每个类型都有其特定的值。属性类型由一个 16 位字表示，其最高位(第 15 位)指明该属性是一种基本属性(最高位为 1)，基本属性格式如图 3-26(a)所示，变长属性格式如图 3-26(b)所示。

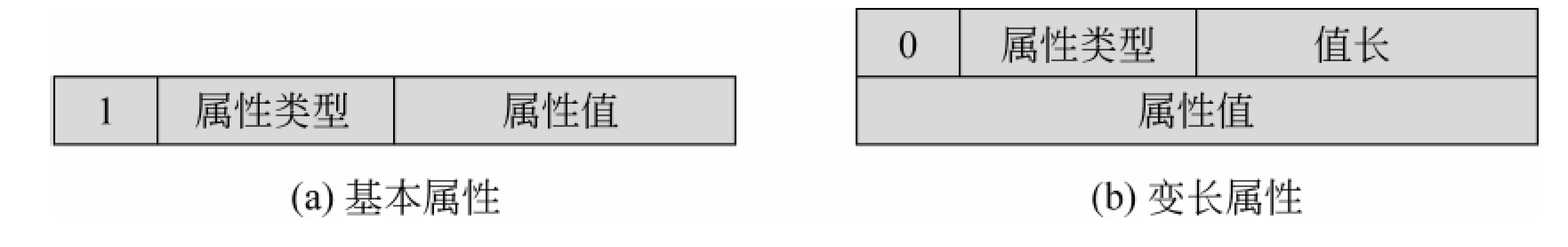


图 3-26　属性格式

ISAKMP 的载荷属性类型如表 3-5 所示。

表 3-5　ISAKMP 的载荷属性类型

分　类	分配的值	长度	分　类	分配的值	长度
SA 生存类型	1	定长	密钥长度	6	定长
SA 生存期	2	变长	密钥轮数	7	定长
组描述	3	定长	压缩字典长度	8	定长
封装模式	4	定长	私有压缩算法	9	变长
认证算法	5	定长			

2. 策略协商

要建立一个共享的安全关联，必须首先协商好所采用的安全策略。安全策略可能非常复杂，所以必须采用灵活的解决方式。为此，ISAKMP 同时使用了安全关联、提议载荷及转码载荷等来表示策略。一个安全关联内可能包含了一个或多个提议，而且每个提议可能包含一个或多个转码方式。

（1）安全关联载荷。安全关联载荷的格式如图 3-27 所示。

下一个载荷	保留字段	SA载荷长度
解释域DOI		
条件		

图 3-27　安全关联载荷的格式

每个字段的含义如下。

① 下一个载荷：消息中下一个载荷的标识符。这里不能填入提议载荷或转码载荷的值，因为它们是 SA 载荷的一部分。

② SA 载荷长度：整个 SA 载荷的长度，包括 SA 载荷以及所有与该 SA 载荷相关的提议载荷和转码载荷。

③ 解释域 DOI：针对不同的安全服务，需要使用不同的 DOI 值。如果 DOI 值为 0，则表示它用于 ISAKMP，可以在阶段 2 为任何协议协商 SA；如果 DOI 值为 1，则表示 DOI 定义了如何用 ISAKMP 为 IPSec 服务建立 SA。

④ 条件：变长字段，包含一些必要的信息，为接收方在协商期间确定策略提供参考。

（2）提议载荷。提议载荷的格式如图 3-28 所示。

下一个载荷	保留字段	P载荷长度	
提议号	协议ID	SPI长度	转码数量
SPI			

图 3-28　提议载荷的格式

每个字段的含义如下。

① 下一个载荷：消息中下一个载荷的标识符，其值只能是 0 或 2。如果消息中还有其他提议，则其值为 2；如果该提议是所在 SA 载荷中的最后一个提议，其值为 0。

② 载荷长度 P：整个提议载荷的长度，包括通用头、提议载荷以及所有与该提议载荷相关的转码载荷。如果消息中有多个具有相同提议号的提议载荷，其值只是当前载荷的长度。

③ 提议号：当前载荷的提议号。在与一个 SA 载荷相关的多个提议载荷中，具有相同提议号的提议之间用“逻辑与”构建策略；具有不同提议号的提议之间用“逻辑或”构建策略。

④ 协议 ID：指定当前协商的安全协议。例如 IPSec ESP、IPSec AH 等。

⑤ SPI 长度：安全协议所定义 SPI 的长度。对于 ISAKMP 来说，ISAKMP 头中的发起者 Cookie 和响应者 Cookie 就是 ISAKMP 的 SPI。

⑥ 转码数量：指定与该提议载荷相关的转码载荷数量。

(3) 转码载荷。转码载荷的格式如图 3-29 所示。

下一个载荷	保留字段	T载荷长度
转码号	转码ID	保留字段
SA属性		

图 3-29 转码载荷的格式

每个字段的含义如下。

① 下一个载荷：消息中下一个载荷的标识符。其值只能是 0 或 3。如果消息中还有其他转码，则其值为 3；如果该转码是所在提议载荷的最后一个转码，其值为 0。

② T 载荷长度：整个转码载荷的长度，包括通用头和转码载荷。

③ 转码号：当前载荷的转码号。与同一个提议载荷相关的多个转码载荷具有不同的转码号。

④ 转码 ID：为当前提议载荷中的协议指定转码标识符。这些转码由 DOI 定义，并依赖于正在协商的协议。

⑤ SA 属性：由转码定义的 SA 属性，这些属性是用前面提到的“属性/值”表示的。

3. 策略协商举例

下面通过两个具体例子说明如何利用 3 种载荷表示安全策略。

(1) 例子 1。假如一个安全策略要求使用 ESP 加密，加密算法可以是 3DES 或 DES；同时使用 AH 认证，认证算法是 SHA。

该策略的 ISAKMP 消息格式如图 3-30 所示。

(2) 例子 2。假如一个安全策略如下。

选择 1：使用 AH 认证，认证算法是 MD5，并且使用 ESP 加密，加密算法是 3DES。

选择 2：使用 ESP 加密，加密算法是 3DES 或 DES。

SA载荷	下一个头=10	保留	载荷长度	
	解释域			
	条件			
提议载荷1	下一个头=2	保留	载荷长度	
	提议号=1	协议ID=ESP	SPI长度	转码数量=2
	SPI			
转码载荷1	下一个头=3	保留	载荷长度	
	转码号=1	协议ID	保留	
	SA属性(加密算法/3DES)			
转码载荷2	下一个头=0	保留	载荷长度	
	转码号=2	协议ID	保留	
	SA属性(加密算法/DES)			
提议载荷1	下一个头=0	保留	载荷长度	
	提议号=1	协议ID=AH	SPI长度	转码数量=1
	SPI			
转码载荷1	下一个头=0	保留	载荷长度	
	转码号=1	协议ID	保留	
	SA属性(认证算法/SHA)			

图 3-30　例子 1 的 ISAKMP 消息格式

该策略的 ISAKMP 消息格式如图 3-31 所示。

3.6　Linux 2.6 内核中 IPSec 的实现分析

1. 套接字缓冲区(sk_buff)对 IPSec 的支持

sk_buff 是网络处理中一个重要的数据结构，在协议栈处理中作为收发数据的载体，协议栈各层次都和该数据结构密切相关。

外出数据包 sk_buff 中有 dst_entry 链表来记录应用于该数据包的 IP 路由。Linux 2.6 内核中 dst_entry 提供对 IPSec 处理的支持——dst_entry 不仅记录 IP 路由信息，还记录查询安全策略数据库(SPD)的结果，使得 IP 数据包在外出之前，先接受安全协议的处理。在本节中，起这样作用的 dst_entry 称为“安全处理目的入口”。一个“安全处理目的入口”可以表达为使用一个安全关联(SA)对数据包进行一次安全处理，如果存在多个 SA，则使用“安全处理目的入口”链表来描述。

进入数据包的 sk_buff 中的 sec_path 类型成员变量 sp(包含指向 SA 的指针数组)记录了在 IPSec 进入处理过程中，依次应用于数据包处理的 SA 及其相关信息，用于以后跟策略相比较，验证已执行的 IPSec 进入处理是否正确。sec_path 及相关结构在/usr/src/linux/include/net/xfrm.h 中定义。sec_path 中 SA 的位置与安全策略中记录的 SA 顺序一致。

SA载荷	下一个头=10	保留	载荷长度	
	解释域			
	条件			
提议载荷1	下一个头=2	保留	载荷长度	
	提议号=1	协议ID=AH	SPI长度	转码数量=1
	SPI			
转码载荷1	下一个头=0	保留	载荷长度	
	提议号=1	协议ID	保留	
	SA属性(认证算法/MD5)			
提议载荷1	下一个头=2	保留	载荷长度	
	提议号=1	协议ID=ESP	SPI长度	转码数量=1
	SPI			
转码载荷1	下一个头=0	保留	载荷长度	
	提议号=1	协议ID	保留	
	SA属性(加密算法/3DES)			
提议载荷2	下一个头=0	保留	载荷长度	
	提议号=2	协议ID=ESP	SPI长度	转码数量=2
	SPI			
转码载荷1	下一个头=3	保留	载荷长度	
	转码号=1	协议ID	保留	
	SA属性(加密算法/3DES)			
转码载荷2	下一个头=0	保留	载荷长度	
	转码号=2	协议ID	保留	
	SA属性(加密算法/DES)			

图 3-31 例子 2 的 ISAKMP 消息格式

2. XFRM 模块

2.5 版之后的内核引入了一种新的 IP 包处理的网络框架，称为“可叠放目标(stackable destination)”堆结构和 XFRM，此设计中的 IPv4 和 IPv6 共享 SPD 和 SAD。

“可叠放目标”是指 dst{}结构链，这些 dst{}是临时建立并有其缓存，一个 dst{}可以插入到原 dst{}前，构成一个堆式结构。每个 dst{}通常都有一个指针指向 xfrm_state{}结构，xfrm_state{}中有数据包的传输处理函数。

XFRM 是处理 IP 数据包的一个新的网络框架，它实际是 IPSec 的 SPD/SAD 管理模块，又与原网络框架的路由和网络数据处理密切关联。

XFRM 代表传输(transformer)，其中定义了两个结构，xfrm_policy{}表示 IPSec SP(Security Policy)和 xfrm_state{}表示 IPSec SA。xfrm state{}通过 xfrm_templ{}和 xfrm_policy{}关联，SPD 由 xfrm_policy{}结构链组成，SAD 由 xfrm_state{}结构链组成。

在 IPSec 的外出处理过程中，会依次调用 xfrm_lookup()、xfrm_tmpl_resolve()、

xfrm_bundle_create()和 dst_output()。xfrm_lookup()在 SPD 中查找 xfrm_policy{},此时栈中的 dst{}指向原 dst{}结构;然后 xfrm_lookup()调用 xfrm_tmpl_resolve,从 xfrm_policy{}中解析得到 xfrm_tmpl{}结构,xfrm_tmpl{}中包含了数据包的处理方式,并查找与 xfrm_tmpl{}匹配的 xfrm_state{},这相当于查找与 IPSec 策略对应的 SA 或 SA 束。xfrm _bundle_create 创建堆叠式目标和 SA 束。以上 3 个函数的过程在路由解析中完成。数据包建立后调用 dst_output(),此时 dst{}结构中外出例程函数指针指向的外出处理函数被调用,外出函数从 sk_buff{}的 dst{}中可得到 xfrm_state{},其结构和函数调用关系如图 3-32 所示。

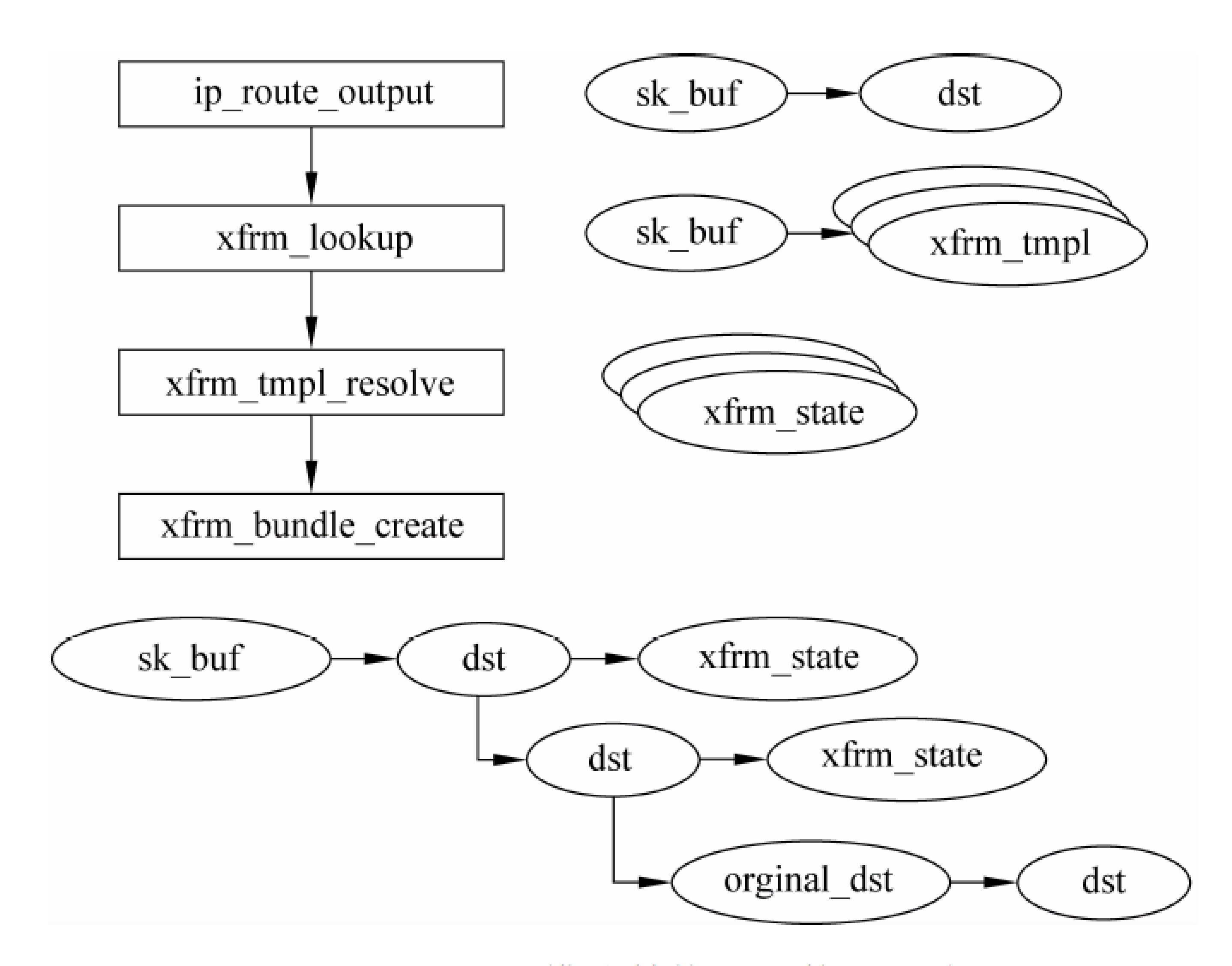


图 3-32　XFRM 模块结构和函数调用关系

net/xfrm/xfrm policy.c 文件中给出了包含 6 个链的策略链表,即策略库的定义如下:

```
struct xfrm_policy xfrm_policy_list
```

3. 数据包的 IPSec 处理

(1) 进入处理。根据源/目的地址、服务类型、进入设备接口索引值,在路由缓存 rt_hash_table 中快速寻找路由,若未找到,则调用 ip_route_input_slow,到 FIB 中查找,并构建结构体 struct flowi{}(flowi 包括源/目的地址、服务类型、进入设备接口索引值等)。ip_local_deliver_finish 中先调用 xfrm4_check_policy,进行进入策略检查,若策略检查不通过,则丢弃该数据包;再调用 ipprot->handler(skb),即传输层的处理函数,这些函数包括 xfrm4_rcv、tcp_rcv、udp_rcv 和 ipip_rcv 等。xfrm4_rcv 调用 xfrm_rcv_encap,xfrm_rcv_encap 中先得到 SPI,根据 SPI 调用 xfrm_state_lookup,找到对应的 SA 束,并进行 SA 有效状态的检测、窗口重放检测、SA 生命期的检测,再进入 AH 和 ESP 的处理,SA 记录在 skb 中,以备后面策略检查使用。

IPSec 处理完后,数据包将作为普通的报文传给上层协议,进行继续处理。上层协议进入策略检查模块处理,根据 skb 中所记录的 SA 信息来验证策略。如果策略通过则继

续;如果没有通过,则丢弃该报文。ipip_rcv 处理隧道模式的数据包,解开外层的数据包后再放入数据包接收队列中。

(2) 转发处理。如图 3-33 中间部分所示。首先进入转发策略检查,若不通过则丢弃,xfrm4_route_forward 进行转发路由和策略查找,xfrm_lookup 查找策略,并找到相应的 SA 或 SA 束。最后,ip_forward_finish 调用 dst_output,将数据转发出去。

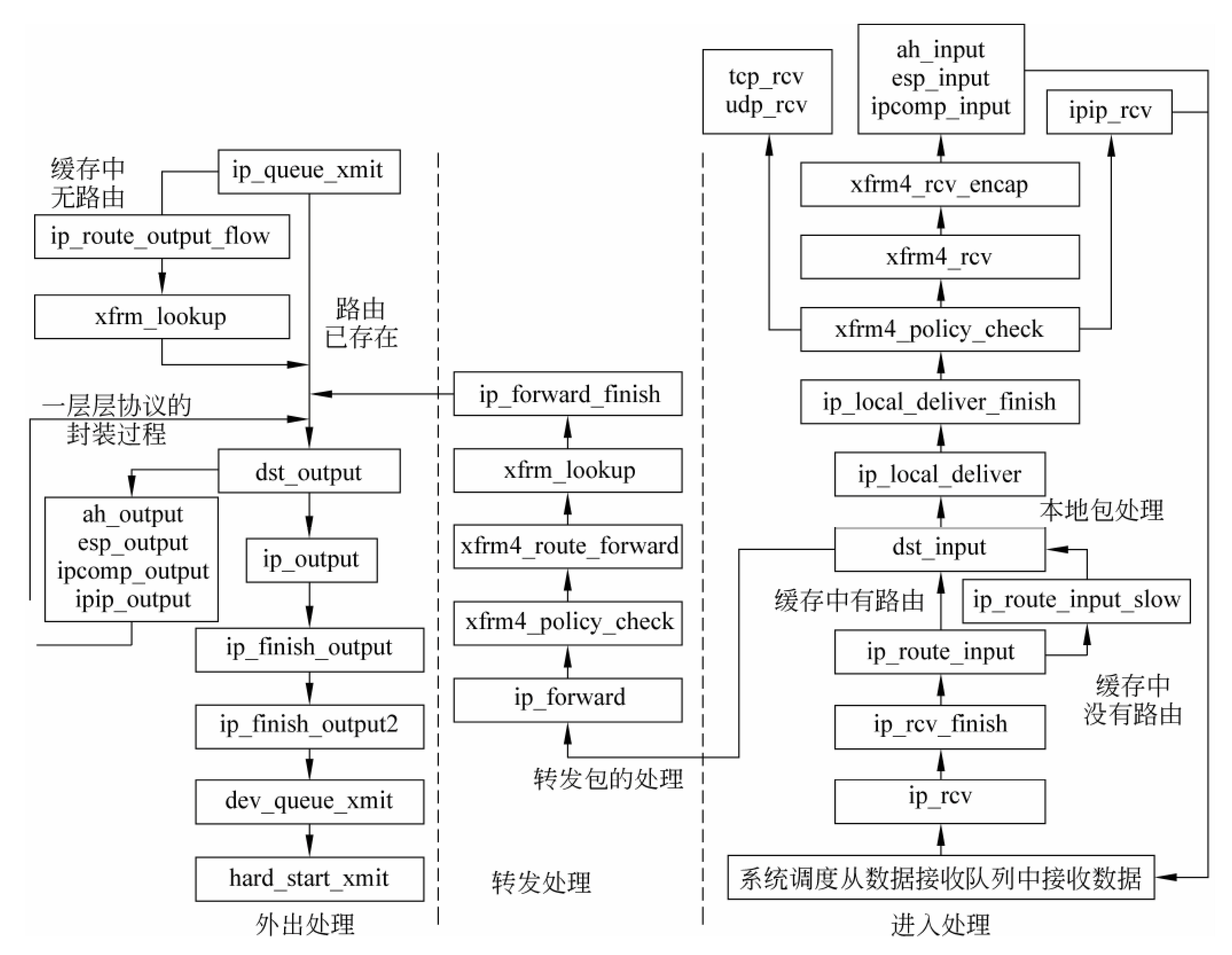


图 3-33 2.6 版内核中 TCP/IP 协议栈数据包处理的流程图

(3) 外出处理。如图 3-34 左边部分所示。首先在路由缓存表中查找路由,若无则调

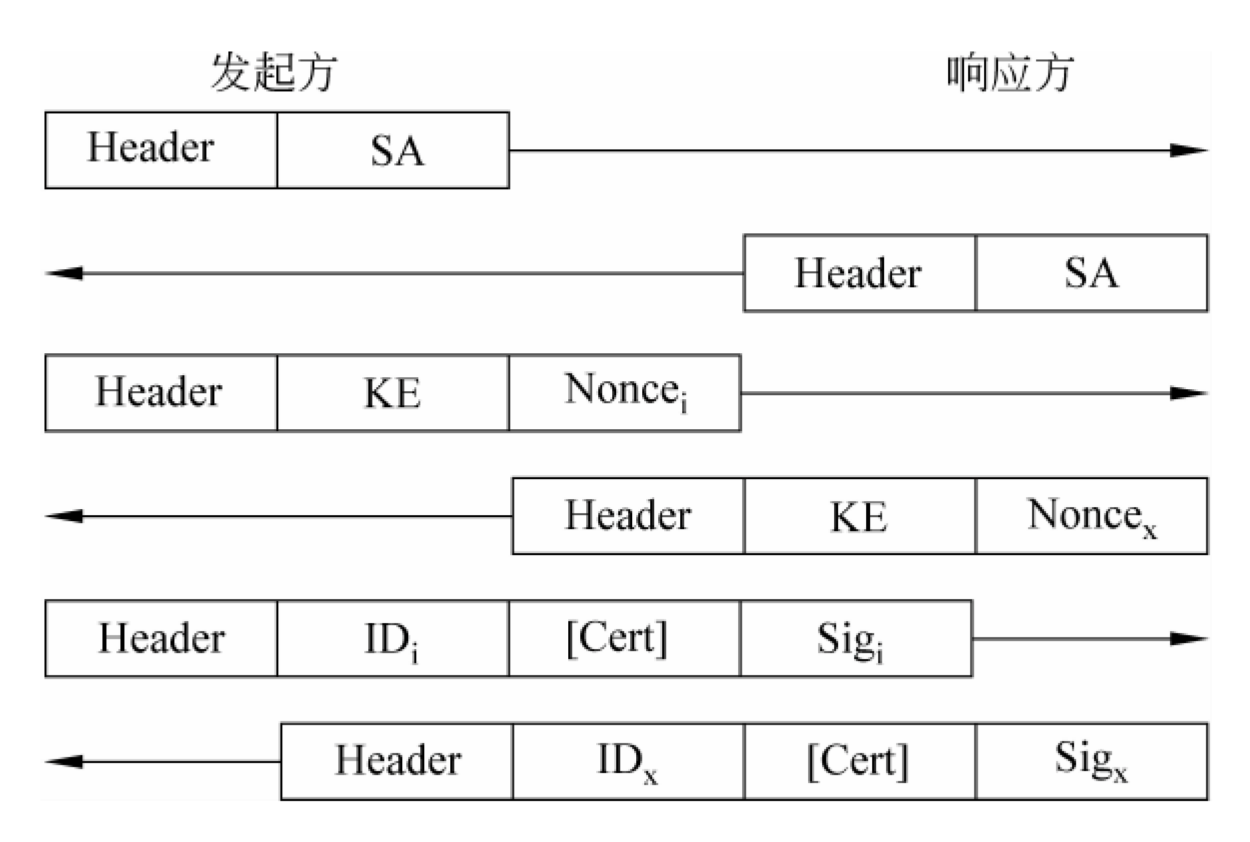


图 3-34 IKE 主模式交换消息头

用 ip_route_output_flow，在 FIB 中查找路由，并调用 xfrm_lookup 查找 IPSec 策略及与策略对应的 SA 或 SA 束，这样就创建了 skb 的 dst 束；dst_output 调用 dst 束中每个 dst 的 output 函数，循环处理，直到遍历 dst 束中的每个 dst，最后由原 dst 的外出函数 ip_output 发送数据包，此时的数据包已经过了 IPSec 的处理，封装成另一 IP 数据包了。

（4）CryptoAPI。CryptoAPI 为 AH/ESP 进入和外出处理提供 DES、3DES、AES 和 Blowfish 加密算法，HMAC、MD5 和 SHA 摘要算法。

3.7 IPSec 协议安全性分析

IPSec 协议的安全特性基本上解决了前述 8 种网络攻击行为，但一些特殊的攻击还是能够实现。

1. 利用 IPSec 进行重放攻击

防重放工作原理是通过丢弃序列号早于本地滑动窗口中最小的序列号分组来实现：在一对一通信时，首先双方建立 SA。然后由发送方生成每个数据包的序号，为防重放做好必要的准备。最后通过接收方利用滑动窗口技术来实现防重放服务。发送方对输出包的处理分为 4 个步骤：查询 SA、生成序号、计算 ICV 和分片。发送方的计数器在建立 SA 时被初始化为 0。发送方不断增加该 SA 的序号，并向“序号”字段中插入新的值。这样，用给定的 SA 所发送的第一个数据包的序号就为 1。发送方通过检查，以保证计数器在插入新值前没有出现循环。如果计数器出现循环，那么发送方就会建立一个新的 SA 和密钥。接收方对输入包的处理分为 4 个步骤：重组、查询 SA、校验序号和校验 ICV。建立 SA 时，接收方的包计数器初始化为 0，然后每接收一个数据包，都要首先检查序号是否出现重复。接收过程主要应用了滑动窗口技术。在这里，窗口大小的最小值为 32，默认值为 64，接收方也可以选择其他值。窗口的最大值表示当前 SA 下有效的最大序号，窗口的最小值表示当前 SA 下有效的最小序号，两者之差为窗口大小。而数据包“序号”字段中的值如果小于窗口容器的最小值，该包就会被丢弃。只有数据包序列号大于窗口最小值，才会继续检查其 ICV，如果 ICV 检查通过，就更新滑动窗口，即下一个可以接受的序列号范围，继续接收后面的数据包。因为序号比目前滑动窗口的最小序号还小的包是已经接受过的包，即为重放的包，而这些包又都被丢弃，这样就防止了重放攻击。

IPSec 协议的一些重要特性如下。

（1）在安全关联中，不包括源地址，每个安全关联（SA）都由一个 3 元组＜SPI，目标地址，所用协议＞唯一标识。其中，安全参数索引用于区别具有相同目标地址和相同协议的不同 SA；目标地址表示该 SA 下接收方的 IP 地址，当前只能是单播地址；所用协议是指选用了 AH 还是 ESP，二者必须并且只能选择其一。但是安全关联中并不包括任何与源地址有关的信息。

（2）对特殊 ICMP 报文建立 SA 后，不检查源地址是否匹配，虽然安全关联中不包括任何与源地址有关的信息，但是在建立 SA 之后，本地策略会确定一个 SA 选择器，还要检查数据包中的源地址与 SA 选择器是否匹配，这样才可保证源验证。但是对由路由器

生成的受 AH 或 ESP 保护的 ICMP 错误消息而言，只能为这种消息报文建立隧道模式的 SA，而且此时并不检查这种 ICMP 报文中的源地址是否与 SA 选择器相匹配。

(3) 当建立 SA 时，通信双方的序号计数器都要被始化为 0。

利用以上特性，下面两种方法可以实现对 IPSec 的重放。

(1) 简单实现。在多对一的通信中，让多个发送方都与接收方之间建立同一个 SA，就可以简单实现对 IPSec 的重放。假设 A 和 B 是发送方，C 为接收方，其工作过程如下：A 与 C 建立 SA，双方计数器归 0，正常收发若干报文，C 的计数器达到某一值；B 截获到 A 发送给 C 的若干报文，这些报文具有一定的序号；B 与 C 建立同一个 SA，此时 C 的计数器将再次归零；B 把所截获的报文重放给 C，这些报文的序号就会落在 C 的滑动接收窗口的内部或右侧，而不会被认为是重放的报文。但通过源验证，就可以知道是谁在进行重放攻击。

(2) 利用 ICMP 错误报文实现。如果利用对 ICMP 错误报文，在隧道模式下建立 SA 来实现对 IPsec 保护之下报文的重放，就无法通过源验证确定谁在进行重放。因为在对这种特殊的 ICMP 报文进行处理时，并不检查源地址，也就无法实现源验证。具体过程如下：捕获在隧道模式下建立 SA 的 ICMP 错误报文；与攻击目标之间建立相同的 SA；重放数据包，对目标实施重放攻击。

实现攻击最重要的一点就是建立了相同的 SA。但是在工程实现中，除非工程师的懒惰，否则很难出现多对一通信建立了相同的 SA。最简单的解决方法就是给 SA 加一个锁，当该 SA 正在使用时，不允许建立该 SA。

2. IKE 主模式交换过程中存在问题，使得拒绝服务攻击有机可乘

主模式交换提供了身份保护机制，经过 3 个步骤、6 个消息。头两个消息协商策略；中间两个消息交换 Diffie-Hellman 的公共值和必要的辅助数据；最后的两个消息验证 Diffie-Hellman 交换。

在图 3-34 中，Header 表示 ISAKMP 头；SA 表示安全关联载荷；KE 表示密钥交换载荷；$Nonce_i$ 表示发起者的 Nonce 载荷；$Nonce_x$ 表示响应者的 Nonce 载荷；ID_i 表示发起者的标识；ID_x 表示响应者的标识；Cert 和 Sig 标识了认证具体机制。

但是，IKE 主模式交换过程中的前 4 个消息都没有加密，这些消息就可以被监听，从而读取并分析该消息的内容。

IKE 主模式交换的双方对收到消息的有效性判断存在问题。例如，第一个消息包含了一个封装有建议载荷的 SA 载荷，并且建议载荷中又封装了多个变换载荷。发起者按照一定的方式产生了一个 Cookie 值 X，并将 X 填充到 ISAKMP 头的发起者 Cookie 域中，由于是第一个消息，响应者 Cookie 域中为 0。如果给发起者发第二个消息，发起者判断有效性的依据有两个，首先是看收到的数据中发起者 Cookie 值是否和第一个消息中发起者 Cookie 值相同；其次看第二个消息中变换载荷的 SA 属性是否与第一个消息中提议的变换载荷的一个或者多个 SA 属性相同。如果这两个条件满足，则发起者就认为收到的第二个消息是有效的，并接受。

同理，后面的第 3 个消息和第 4 个消息也有类似问题。

当然，这种监听消息，然后伪造下一个消息的办法，在实际生产中的成功率还是相对比较低的。但是，一些实验室环境的实验表明，这样的想法是可行的，并且找到了具体的方法，能有效破坏特定 IPSec 通信的安全关联建立，成功率达到 95%。

要解决这个安全隐患，可以对每个消息中的关键内容进行加密处理，例如，在消息中的发起者 Cookie。

习题 3

一、填空题

1. IPSec 安全体系结构由________、________和________3 个主要部分组成。
2. 在安全关联数据库中，对任何进入或外出的数据包有________、________和________3 种处理选择。

二、选择题

1. ________协议是一个用于提供 IP 数据包完整性、身份认证和可选的抗重播保护的机制，但不提供数据机密性保护。

A. AH 协议　　B. ESP 协议　　C. IPSec 协议　　D. PPTP 协议

2. 不属于针对 IPSec 攻击的是________。

A. 实现方式攻击　　B. 密钥管理攻击
C. 客户机攻击　　D. 攻击 GRE

三、判断题

1. AH 协议为 IP 数据包提供了数据完整性服务，AH 不仅为上层协议提供认证，还可以为 IP 头所有字段提供认证。　　(　　)
2. 在使用 IPSec 保护一个 IP 数据包之前，必须建立一个 SA，在自动建立 SA 时，要使用 IKE 协议，IKE 协议是专为 IPSec 协议开发的必要交换协议。　　(　　)
3. IPSec 协议是完美的安全协议，解决了网络层协议的所有安全问题。　　(　　)
4. 当一个数据包达到隧道端点时，则要使用一个三元组＜源 IP 地址；IPSec 协议类型；SPI＞，在 SAD 中查找用于处理该数据包的 SA。　　(　　)
5. 安全关联(SA)是双向的，为了保证两个主机或两个安全网关之间双向通信的安全，只需建立一个 SA。　　(　　)

四、思考题

1. 在 IPSec 协议中，用户是如何定义和协商 SA 的？又是如何查找和定位 SA 的？
2. ESP 协议会出现像 AH 协议在网络传输中不适用的情况吗？

五、分析题

已知 SA 载荷、提议载荷和转码载荷的格式如图 3-35 所示，请根据策略给出

ISAKMP 报文，要求使用 ESP 加密，加密算法可以是 3DES 或 DES；或者使用 AH 认证，认证算法是 SHA。

SA 载荷格式

下一个载荷	保留	SA 载荷长度
解释域		
条件		

提议载荷格式

下一个载荷	保留	P 载荷长度	
提议号	协议 ID	SPI 长度	转码号
SPI			

转码载荷格式

下一个载荷	保留	T 载荷长度
转码号	转码 ID	
SA 属性		

图 3-35　SA 载荷、提议载荷和转码载荷的格式

第 4 章　传输层安全协议

4.1　背景介绍

随着 Internet 的迅猛发展和日益普及，传统的办公和交易方式已经逐渐退居二线，人们已经越来越习惯于通过网络进行各种各样的网上办公和在线交易。这就要求为网上金融、网上银行、网上证券、电子商务、电子政务、网上交税、网上工商等多种网上办公、交易提供完备的安全服务功能，保证个人隐私信息，诸如身份信息、银行卡密码、电话号码、家庭住址等，在交互的过程中不至于发生泄露，而仅为交易的双方所见。因此，在此类应用中，如何保证机密性、完整性、身份鉴别、不可否认性，成为用户的迫切需求。遗憾的是，通用的 HTTP、FTP、电子邮件等协议都无法满足这些安全需求。当然，我们可以为每个应用层协议单独增加安全功能，但对于种类繁多且数量巨大的应用协议来说，这么做显然是不现实的。既然高层数据都必须通过低层封装，就可以通过解决低层传输层安全性的问题，一揽子解决高层应用的安全问题。

传输层安全协议（Transport Layer Security Protocol，TLS）正是为了解决传输层安全问题而提出的。传输层安全性就是要保证因特网上任意两个主机进程之间数据交换的安全性，包括建立连接时的用户身份合法性、数据交换过程中的数据机密性、数据完整性以及不可否认性等方面。传输层安全协议增强了传输层协议的安全性，它在传输层协议的基础上增加了安全协商和数据加密/解密处理等安全机制和功能。现实中，大多数用户通常选择使用的传输层安全协议是安全套接字层（Secure Sockets Layer，SSL）协议，通过 SSL 协议对用户隐私数据进行适当加密的形式来实现保护。SSL 协议对于用户而言是透明的，普通用户使用 SSL 进行网络连接的区别不外乎是浏览器地址栏中的 URL 地址是以 https 作为开头，地址栏最右端或状态栏会有一个挂锁或钥匙的图标。

实际上，SSL 是一个独立于平台和应用的协议。图 4-1 显示了 SSL 在协议栈中的位置，用于保护基于 TCP 的应用，SSL 在 TCP 层之上、应用层之下，就像 TCP 连接的套接字一样工作。简单来说，SSL 在访问端和被访问端，或应用端和服务器端之间建立一条相对独立的、安全的通道，并利用自身的数学加密算法，对来往的信息进行严格加密，从而保证数据在此通道内传输时拥有足够的安全性。SSL 协议提供了 3 种安全特性，内容如下。

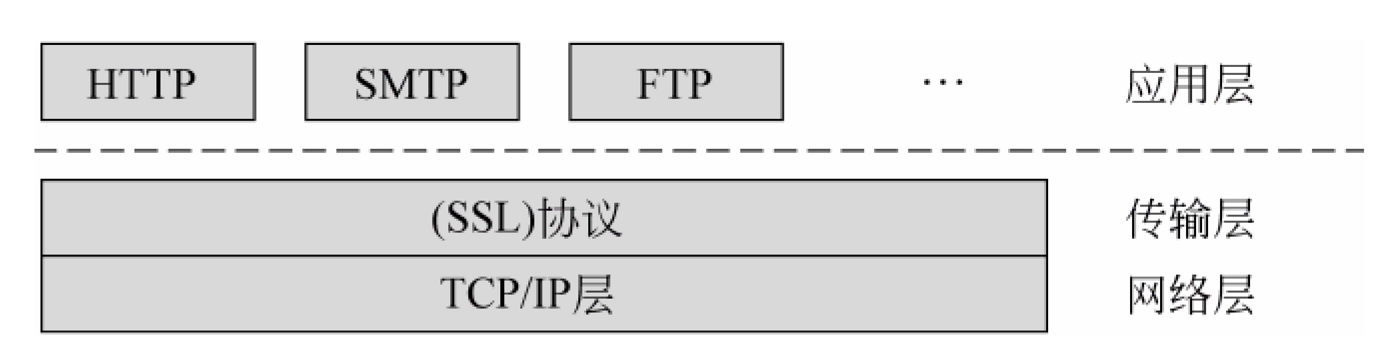


图 4-1　SSL 协议在协议栈中的位置

(1) 数据机密性：采用对称加密算法来加密数据，密钥是在双方握手时协商指定的。

(2) 数据完整性：采用消息鉴别码(MAC)来验证数据的完整性，MAC 是采用 Hash 函数来实现的。

(3) 身份合法性：采用非对称密码算法和数字证书来验证通信实体的身份合法性。

SSL 协议的基本目标是在两个通信实体之间建立安全的通信连接，为基于客户机/服务器模式的网络应用提供安全保护。图 4-2 给出了一个典型基于 SSL 的 VPN 应用，展示一个高校研究人员如何通过 Web 浏览器或专用客户端安全访问内部资源。首先，校园网内部的资源服务器向外网用户提供一个虚拟的 URL 地址，当用户从外网访问校园网内网资源时，发起的连接被 SSL VPN 网关取得，依据安全控制策略，为分散移动用户提供从外网访问企业内网资源的安全访问通道，并通过认证后映射到不同的应用服务器。采用这种方式能够屏蔽内部网络的结构，不易遭受来自外部的攻击。

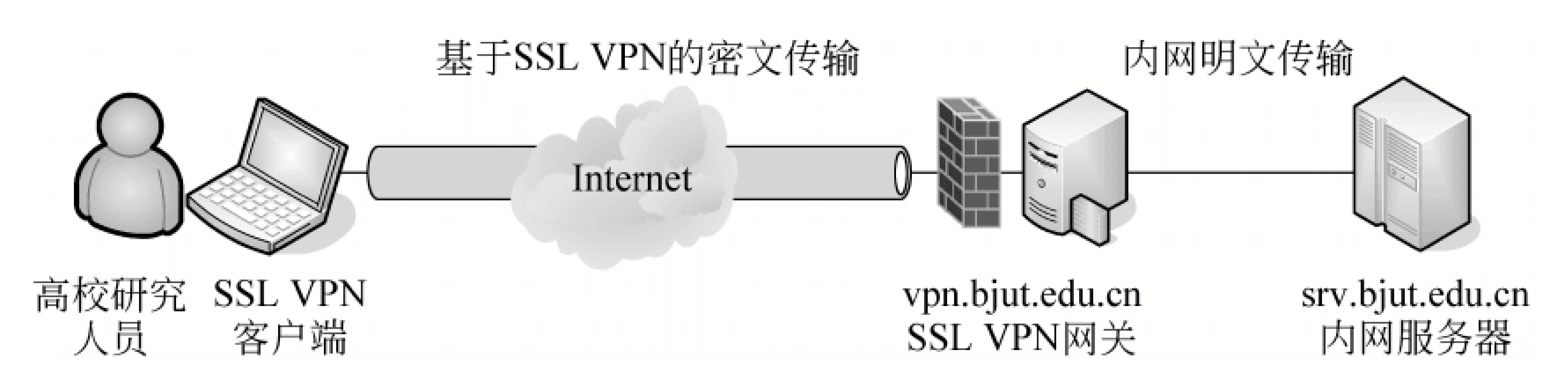


图 4-2　高校科研人员利用 SSL VPN 访问内网资源

SSL 协议最初是由网景通讯公司(Netscape Communications Corporation)开发的一种用于数据加密及身份认证的通信协议，并成功地应用于 Netscape Navigator 浏览器，与其他软件一起组成 Netscape Communicator 商业套件。SSL 历经多次修改，最早的版本是 1994 年推出的 SSL v1.0 版本，同年 11 月，SSL v2.0 版本首次公开，并集成在 Netscape Navigator 浏览器中。SSL v3.0 版本是这一系列的最新版本，于 1996 年推出，并成为应用最为广泛的版本。随后，更多的科研单位、大学、公司加入了 SSL 协议的相关研究开发工作，形成了一系列国际标准。互联网标准规范制定的最主要组织——Internet 工程任务组(Internet Engineering Task Force，IETF)下辖的传输层安全工作组(Transport Layer Security Working Group，TLSWG)，从 1996 年建立开始就致力于传输层安全协议的标准化工作。TSG 工作组从 SSL v3.0 版本开始，不断发展形成了传输层安全协议标准 TLS v1.0 和 TLS v1.1 版本。除此之外，TLS 工作组也对适用于 SSL 协议的数据加密方法进行了研究。目前，TLS 的最新版本是 2008 年 8 月公布的 1.2 版，它的最大变化是去除了协议对 MD5 和 SHA-1 摘要算法的依赖性，同时避免对 1.1 版本进行无谓修改。时至今日，SSL 协议的内容还在不断发展和扩充，包括寻找新的 TLS 认证加密模式等。TLS 协议族最近一次的更新时间是 2010 年 2 月，对客户端和服务器交互过程中的重新协商方式进行了修订。

值得注意的是，由于 SSL 受制于版权保护和专利壁垒，以及加密算法的限制，不少用户开始转而使用 OpenSSL。OpenSSL 是开放源码的 SSL 套件，是以 Eric A. Young 和 Tim J. Hudson 两人所写的 SSLeasy 为基础发展起来的。它的目标是开发一个健壮的、商业级的、完整的开放源代码的工具包，用加密算法来实现安全的 Socket 层和传输层的

安全性。它包含了完整的加密算法、数字签名算法及证书算法等，可以很好地保证数据的完整性、保密性和正确性。OpenSSL 采用 C 语言作为开发语言，使得 OpenSSL 具有优秀的跨平台性能。OpenSSL 支持 Linux、Windows、BSD、Mac、VMS 等平台，使得 OpenSSL 具有广泛的适用性。OpenSSL 可以用于商业用途，但是使用者应该考虑自己所使用的算法有没有受到本国专利的限制。OpenSSL 可以作为 SSL 的替代方案，由于它是完全免费和开放源代码的，且易于二次开发，预计 OpenSSL 的使用将会越来越多。

4.2　SSL 协议简介

SSL 协议的主要目的是保障两个应用间通信的私密性和可靠性。SSL 协议提供传输协议之上的可靠的端到端安全服务，为两个通信对等实体之间提供机密性、完整性和身份鉴别服务。

SSL 协议是一个分层协议，由两层组成：SSL 记录协议和 SSL 握手协议，如图 4-3 所示，内容如下。

（1）SSL 记录协议用于封装不同的高层协议，它建立在可靠的传输协议之上（如 TCP 协议）。

（2）SSL 握手协议用于数据交换前服务器和客户端双方相互认证以及密码算法和密钥的协商。

SSL 握手协议还可细分为握手协议、密钥更改协议和告警协议，所以也有资料将 SSL 协议分为 4 层：SSL 记录协议、SSL 握手协议、密钥更改协议和告警协议。这样一来，SSL 的协议栈也可如图 4-4 所示。

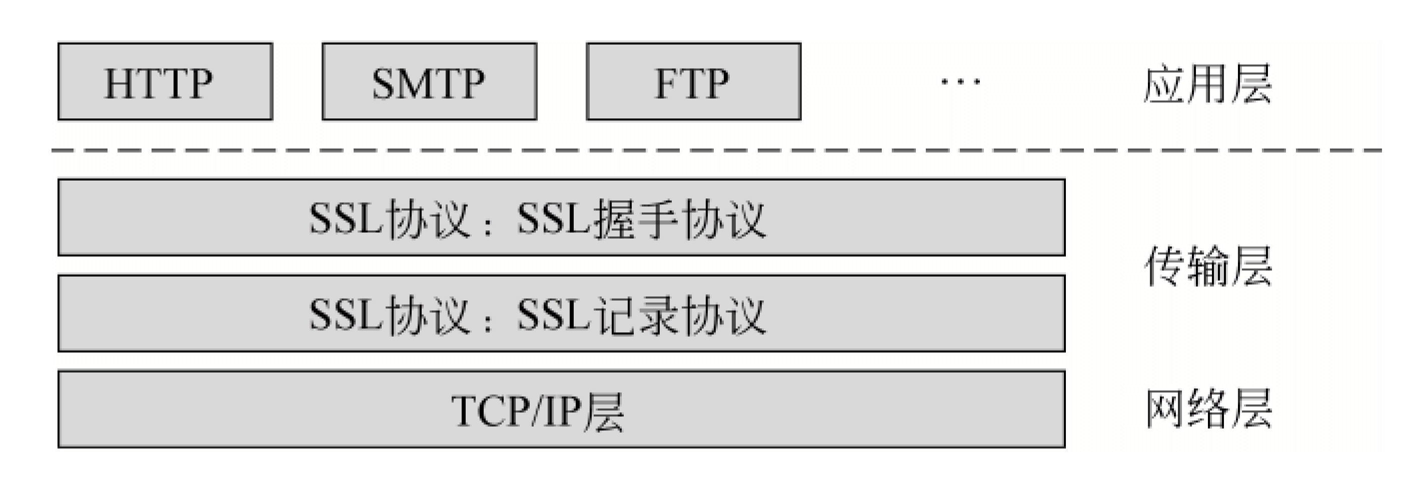


图 4-3　SSL 两层协议的层次结构示意图

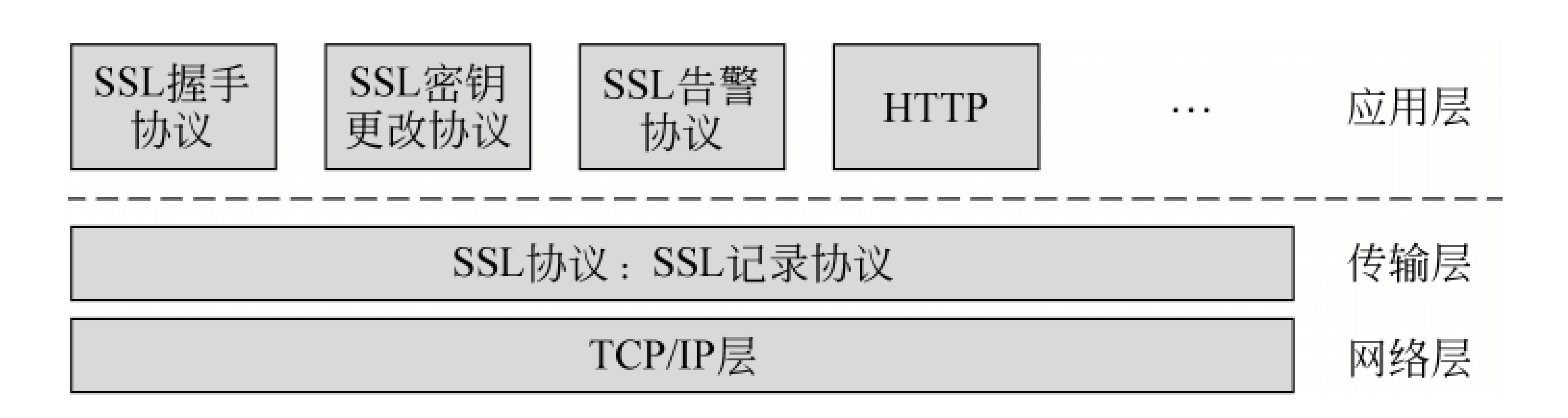


图 4-4　SSL 四层协议的层次结构示意图

SSL 协议独立于应用层协议，高层协议可以在 SSL 协议层之上透明传输。SSL 协议有以下 3 个基本性质。

（1）保障连接的私密性。初次握手协商好密钥后，即可通过对称加密方法（如 DES、

RC4 等)进行数据加密,保障通信连接的私密性。

(2) 通信实体间身份鉴别。通信实体能够通过非对称加密或公钥加密方法(如 RSA、DSS 等)进行身份鉴别。

(3) 保障连接的可靠性。协议通过 MAC 算法保证传输消息的完整性。SHA、MD5 等安全 HASH 算法可用于 MAC 计算。

接下来将详细介绍 SSL 协议内容。由于 SSL 协议的版本较多,本章的讨论以 SSL v3.0 版本为主,兼顾其他版本的协议内容。

4.3 SSL 握手协议

4.3.1 SSL 握手协议概述

SSL 握手协议工作在 SSL 记录协议层之上,用于协商产生会话状态的加密参数。当 SSL 客户端和服务器首次开始通信时,它们就协议版本、加密算法的选择、是否互相认证进行协商,并使用公钥加密技术产生共享秘密。所有这些工作都是由握手协议完成的,大致可以分为以下两个阶段。

(1) 第一阶段——“密钥等信息交换阶段”。通信双方通过相互发送 Hello 消息进行初始化。通过 Hello 消息,双方就能够确定是否需要为本次会话产生一个新密钥。如果本次会话是一个新会话,则需要产生新的密钥,双方需要进入密钥交换过程;如果本次会话建立在一个已有的连接上,则不需要产生新的密钥,双方立即进入握手协议的第二阶段。

(2) 第二阶段——“用户身份认证阶段”。对用户身份进行认证,通常服务器方要求客户方提供经过签名的客户证书进行认证,并将认证结果返回给客户。

SSL 握手协议的具体工作过程描述如下。

(1) 客户端首先发出客户问候消息(Client Hello Message),服务器收到后,或者发出服务器问候消息(Server Hello Message),或者发出终止错误,并中断连接。客户端和服务器的问候消息将协商产生下列属性:协议版本(Protocol Version)、会话标识符(Session ID)、加密算法(Cipher Suite)及压缩方法(Compression Method),此外还将产生和交换两个随机数 Clienthello.random 和 Serverhello.random。

(2) 客户问候消息发送完后,如果 Server 端需要进行认证,会发送它的证书。另外,如果需要的话(例如,如果它们的服务器没有证书,或者其证书仅用来进行签名),将发出一个 Server Key Exchange 消息。如果 Server 端已经被认证,而且所选的加密算法(Cipher Suite)支持的话,可以向客户端请求证书。在验证以后,服务器就发送服务器问候结束消息(Server Hello Done Message),以示达成了握手协议。

(3) 如果服务器发出一个 Certificate Request 消息,客户端必须发出证书消息(Certificate Message),或者一个 No Certificate 报警。此时,客户端密钥交换消息(Client Key Exchange Message)准备发送,消息的内容将依赖于客户端问候消息(Client Hello

Message)和服务器问候消息(Server Hello Message)所协商选择的公钥算法。如果客户端已经发出了一个具备签名能力的证书,一个数字签名后的证书验证消息(Certificate Verify Message)将被发送,以确认此证书的合法性。

(4) 此时,客户端可以发送密钥更改(Change Cipher Spec)消息,客户端将尚未协商确定的加密算法(Cipher Spec)复制加入到当前加密算法(Cipher Spec)。然后,客户端立即用新的算法、密钥和密钥素材发出结束消息。服务器将发出自己的改变加密规范消息(Change Cipher Spec Message)作为回应,同时将尚未协商确定加密规范复制加入到当前加密规范,并用新的加密规范发出结束消息。

(5) 此时,握手过程结束,客户端和服务器可以开始交换应用加密数据,应用数据加密一般是用第(2)步密钥协商时确定的对称加/解密密钥,如 DES、3DES 等。目前,商用加密强度为 128 位,非对称密钥一般为 RAS,商用强度为 1024 位,用于证书的验证。

完整的 SSL 握手协议消息交换过程如图 4-5 所示。

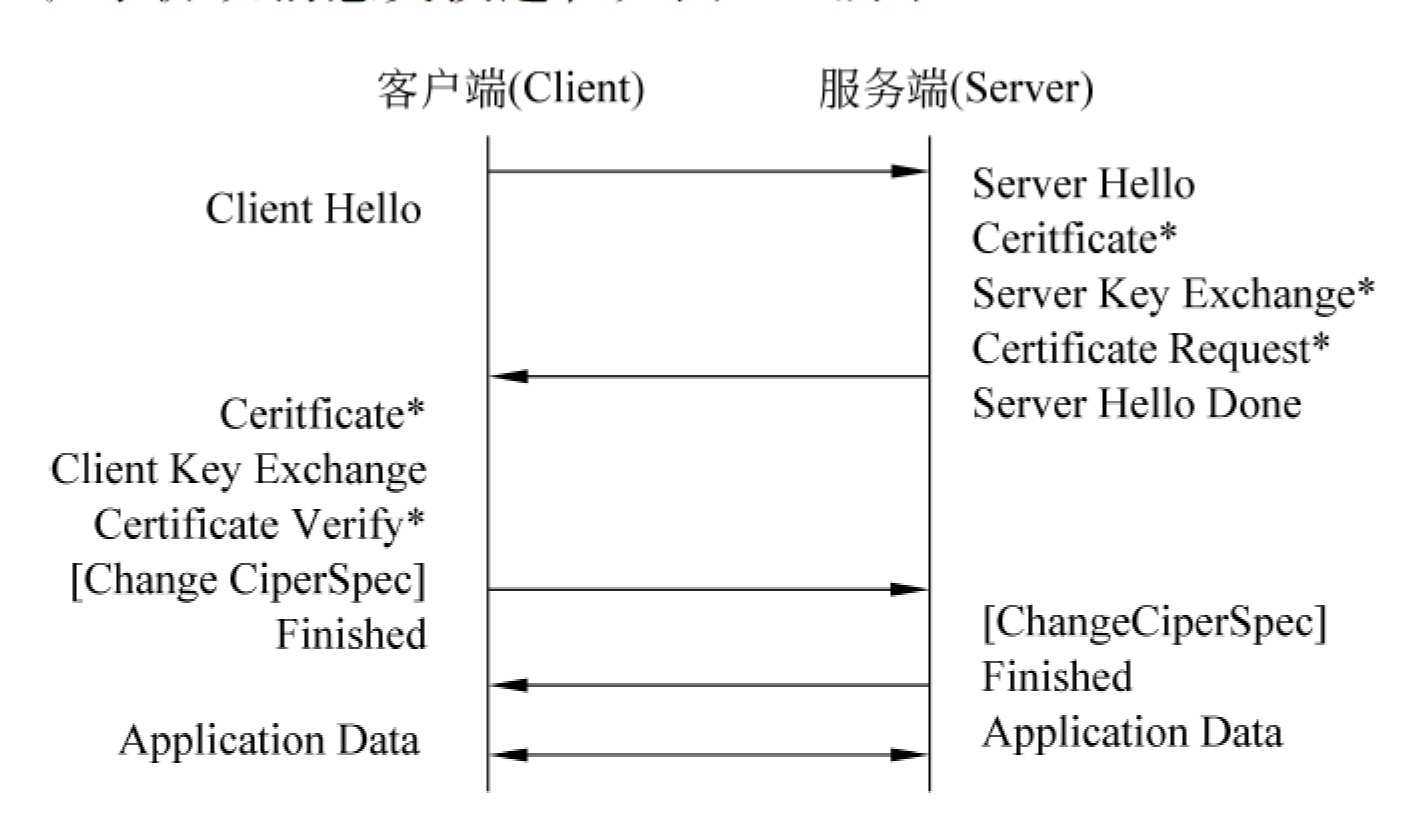


图 4-5　完整的 SSL 握手协议消息交换过程

图中,带 * 号的步骤是可选的,或依据状态而发的消息,而密钥更改(Change Cipher Spec)用于客户端与服务器协商新的加密数据包时而改变原先的加密算法。

如果双方是在已有连接上重建一个会话,则不需要协商密钥以及有关会话参数,可以简化握手协商过程,内容如下。

(1) 客户方使用一个已有的会话标识符(Session ID)发出 Client Hello 消息。

(2) 服务方在会话队列中查找相匹配的会话标示识符(Session ID),如果有相匹配的会话,服务器方在该会话状态下重新建立连接,并使用相同的会话标示识符(Session ID),向客户方发出一个 Server Hello 消息。如果没有相匹配的会话,则服务方产生一个新的会话标识符(Session ID),并且客户方和服务方之间必须进行一次完整的握手协商过程。

(3) 在会话标识符(Session ID)匹配的情况下,客户方和服务方必须分别发送 Change Cipher Spec 消息,然后发送 Finished 消息。

(4) 此时,重建一个会话结束。客户方和服务方进入数据交换阶段。

简化的 SSL 握手协议消息交换过程如图 4-6 所示。

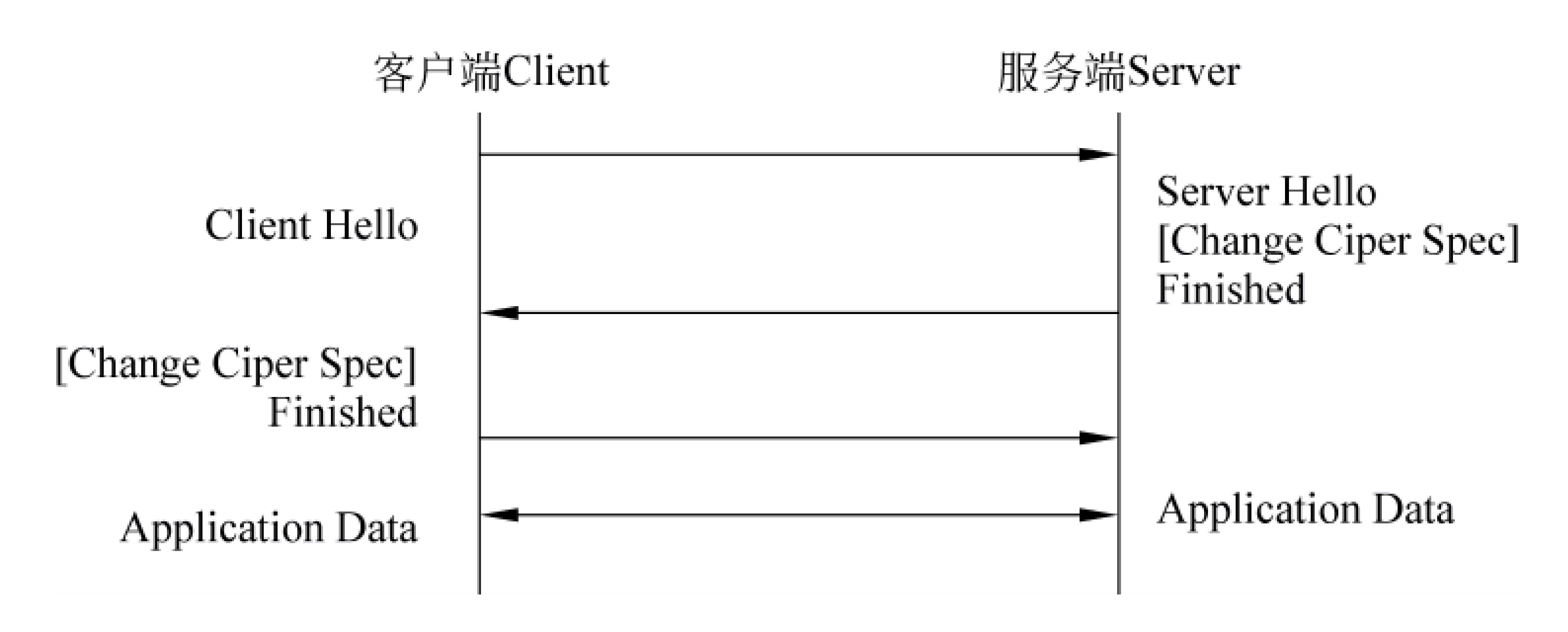


图 4-6 简化的 SSL 握手协议消息交换过程

4.3.2 SSL 握手消息格式

SSL 握手协议由一系列握手消息的交互组成。SSL 握手协议定义了若干握手消息，用于在通信双方之间建立会话和协商安全属性。握手消息将提交给 SSL 记录层，由记录层封装一个或多个 SSL_Plaintext 结构。

SSL 的握手消息格式如表 4-1 所示。

表 4-1 SSL 的握手消息格式

消息名称	消息类型	发送方向	消息名称	消息类型	发送方向
Hello_Request	0	S→C	Certificate_Request	13	S→C
Client_Hello	1	C→S	Server_Hello_Done	14	S→C
Server_Hello	2	C→S; S→C	Certificate_Verify	15	C→S
Certificate	11	S→C	Client_Key_Exchange	16	C→S
Server_Key_Exchange	12	S→C	Finished	20	C→S;S→C

注：S 代表服务端，C 代表客户端

握手协议的消息必须按指定的顺序发出，如若不然，则会导致错误。

1. 问候消息(Hello Message)

Hello 消息用来建立一个会话，以增强客户方和服务方之间信息交换的安全性。当建立一个新会话时，加密算法、Hash 算法和压缩算法等都要初始化为空。

(1) Hello Request 消息。服务器可以在任何时候发送 Hello Request 消息，要求客户方重新开始协商过程。客户方在收到该消息后使用 Client Hello 消息进行响应，同意重新开始协商过程。

在握手协商过程中，如果客户端在进行握手协商，此消息将会被客户端所忽略，不予响应。

(2) Client Hello 消息。当客户端第一次与服务器连接时，必须发客户问候消息(Client Hello)作为它的第一个消息。客户端也可以将此消息作为对服务器发来的问候

请求消息(Hello Reques)的回应,还可以作为在现有的会话连接上主动请求重新协商安全参数的标志发出此消息。

Client Hello 消息结构如下:

```
struct
{
    ProtocolVersion client_version;                    //版本号
    Random random;                                     //随机数
    SessionID session_id;                              //会话 ID
    CipherSuite cipher_suites<2..2^16-1> ;             //加密选项列表
    CompressionMethod compression_methods<1..2^8-1> ;  //压缩算法列表
} ClientHello;
```

其中的参数说明如下。

client_version:客户端希望在此次对话中使用 SSL 协议的版本,应该是被客户端所支持的最新版本。对于本章所描述的 SSL 协议,版本号应该是 3.0。

random:由客户端产生的随机数结构。

session_id:客户端在此次连接中想使用的对话标识符(ID)。当会话 ID 不可用或客户方想要更新安全参数时,会话 ID 为空。

cipher_suites:客户方可以支持的加密算法列表,由客户方按偏好排列(列表的第一项是其最佳选择)。如果会话 ID 非空,则要包含本次会话的加密选项列表。

compression_methods:由客户方按偏好排列(列表的第一项是其最佳选择)。如果会话 ID 非空,则要包含本次会话的压缩算法列表。同时所有实现必须支持 CompressionMethod.null。

继发送 Client Hello 消息之后,客户端等候一个服务器问候消息(Server Hello message)。除了 Hello 消息外,由服务器返回的任何其他握手消息,均被视为致命错误(Fatal Error)。

(3) 服务器问候消息(Server Hello)。服务器处理客户端问候消息(Client Hello),并且对客户端问候消息作出握手失败(Handshake_failure)警告,或者发出服务器问候消息(Server Hello)作出响应。

Server Hello 消息结构如下。

```
struct
{
    ProtocolVersion server version;                //版本号
    Random random;                                 //随机数
    SessionID session_id;                          //会话 ID
    CipherSuite cipher_suite;                      //加密选项列表
    CompressionMethod compression_method;          //压缩算法列表
} ServerHello;
```

其中的参数说明如下。

server_version：服务器方同意使用的 SSL 协议版本，包含客户端在客户端问候消息(client hello)中建议使用的最低版本和被服务器所支持的最高版本。对于本章所描述的 SSL 协议，版本号应该是 3.0。

random：指由服务器产生的随机数结构。必须与客户问候消息中的 ClientHello.random 不同，并且独立于 ClientHello.random。

session_id：指服务器方同意使用的会话 ID。若客户问候消息中的 ClientHello.session_id 非空，服务器将在对话缓存器中寻找匹配的会话。如果找到了匹配的会话，则服务器方使用指定的会话状态建立一个新的连接，并向客户方返回该会话 ID，表示重新激活该会话；否则，向客户方返回一个不同于客户方会话 ID 的新会话 ID，表示启动一个新的会话；服务器也可以返回一个空的会话 ID，表示不能激活一个会话。

cipher_suites：必须是一个与客户方加密选项列表 ClientHello.cipher_suites 中相匹配的密码组。对于重建的会话来说，其值来自于重新激活的会话状态。

compression_methods：必须是一个与客户方压缩算法列表 compress_method 中相匹配的压缩算法。对重建的会话来说，其值来自于重新激活的会话状态。

2. 服务器证书消息(Server Certificate)

如果服务器方确认了一个会话，则在发送 Server Hello 消息之后，立即发送服务器方证书消息。证书类型必须与密码组的密钥交换算法相一致，通常是一个标准的 X.509.v3 证书。对于 Fortezza 算法，则是一个修改的 X.509 证书。客户端证书的类型要与服务器的证书类型相同。

Server Certificate 消息结构如下：

```
struct
{
    ASN.1Cert certificate_list<1..2^24-1> ;
} Certificate;
```

Certificate 消息中包含一个 X.509 证书序列，发送者的证书排在前，认证中心的证书排在后。

3. 服务器密钥交换消息(Server Key Exchange Message)

若服务器没有证书，或只有供其签名用的公钥证书(例如 DSS 证书，只供签名的 RSA 证书)，或使用了 Fortezza/DMS 密钥交换，则服务器发出服务器密钥交换消息(Server Key Exchange Message)。如果服务器方证书中包含了 Diffie_hellman 参数，则不需要发送这个消息。

Server Key Exchange Message 消息结构如下：

```
struct
{
    select (KeyExchangeAlgorithm)
    {
```

```
        case diffie_hellman:
            ServerDHParams params;
            Signature signed_params;
        case rsa:
            ServerRSAParams params;
            Signature signed_params;
        case fortezza_kea:
            ServerFortezzaParams params;
    };
} ServerKeyExchange;
```

其中的参数说明如下。

params：服务器的密钥交换参数。

signed_params t：相应的参数值的哈希值，及对此哈希值的签名。

4. 证书请求消息(Certificate Request)

如果选择的加密算法允许的话，为了满足所选密码组的要求，非匿名的服务器可以向客户发送 Certificate Request 消息，请求客户方确认证书。

客户证书类型可以是如下几种：rsa_sign、dss_sign、rsa_fixed_dh、dss_fixed_dh、rsa_ephemeral_dh、dss_ephemeral_dh、fortezza_dms，由服务器方排序。

Certificate Request 消息结构如下：

```
struct
{
    ClientCertificateType certificate_types<1..2^8-1>;
    DistinguishedName certificate_authorities<3..2^16-1>;
} CertificateRequest;
```

其中的参数说明如下。

certificate_types：此域的值是一被请求的证书类型的列表，此列表是按服务器偏好的先后顺序排序的。

certificate_authorities：可接受的证书认证方唯一名称列表。

5. 服务器问候结束消息(Server Hello Done)

一旦服务器发出 Server Hello Done 消息，表示服务器方完成了握手协商，并等待客户方的回应。客户方在收到 Server Hello Done 消息后，需要检查服务器是否提供了有效的证书，以及 Server Hello Done 消息中的参数是否是可接受的，然后根据检查结果做出适当的回应。

Server Hello Done 消息结构如下：

```
struct { } ServerHelloDone;
```

6. 客户端的证书消息(Client Certificate)

客户端证书消息是客户端收到 Server Hello Done 消息后首先发送的消息,并且只有在服务器端通过 Ceritificate Request 消息请求客户端证书时才发送。如果没有合适的证书,客户端将发出一个 NO_Certificate 警告。此外,客户端的 Diffie-hellman 证书必须与服务器端指定的 Diffie-Hellman 参数相匹配。

7. 客户端密钥交换消息(Client Key Exchange Message)

Client Key Exchange 消息结构如下:

```
struct
{
    select (KeyExchangeAlgorithm)
    {
    case rsa:
        EncryptedPreMasterSecret;
    case diffie_hellman:
        ClientDiffieHellmanPublic;
    case fortezza_dms:
        FortezzaKeys;
    } exchange_keys;
} ClientKeyExchange;
```

其中,密钥交换算法取决于所选择的公钥算法,内容如下。

(1) 基于 RSA 的密钥交换。如果选择 RSA 作为密钥交换算法,客户端将产生一个 48 字节的 Premaster Key,并使用服务器端证书中的公钥或者 ServerKeyExchange 消息中的临时 RSA 密钥,对 Premaser Key 进行加密处理,然后将结果放在 ClientKeyExchange 消息中发送出去。

(2) 基于 FORTEZZA 的密钥交换。在 FORTEZZA 算法中,必须使用 FORTEZZA 密钥交换算法(KEA)和令牌加密密钥(TEA)。客户端首先随机生成一个 48 字节的 Premaster Key 作为会话密码,用 TEA 加密该会话密钥,然后发送到服务器端。在 KEA 算法中,必须同时使用服务器端证书中的公钥和客户端令牌中的私钥。客户端使用自己的私钥来发送公钥。

(3) 基于 Diffie-Hellman 的密钥交换。如果在客户端证书中没有包含 Diffie-Hellman 公共值,则需要向服务器端发送客户方的 Diffie-Hellman 公共值。

8. 证书验证消息(Certificate Verify)

CertificateVerify 消息用来对客户端证书的签名验证,必须跟随在具有签名能力的客户端证书后发送。这种客户端证书可以使用 MD5 或 SHA 算法来签名。除了 Diffie-Hellman 证书之外的所有客户端证书都可通过签名来验证。

Certificate Verify 消息结构如下:

```
struct
{
    Signature  signature;
} CertificateVerify;
```

在这里，握手消息(Handshake_messages)指的是从客户端问候(Client Hello)消息开始的，不包含此消息在内的到目前为止的所有握手消息。

9. 结束消息(Finished)

通常，Finished 消息要在 Changed Cipher Spec 消息之后发送，用来检测密钥交换过程是否完成。收到 Finished 消息后，首先检查其内容的正确性，然后通信双方可以立即开始发送加密后的数据，而不需要对该消息进行确认。如果 Finished 消息没有跟在 Changed Cipher Spec 消息之后发送，则会导致一个致命的错误。

Finished 消息结构如下：

```
struct
{
    opaque md5_hash[16];
    opaque sha_hash[20];
} Finished;
```

其中的参数说明如下：由服务器发出的结束消息中包含的哈希值与 Sender. server 中的值是一致的，而由客户端发出的结束消息中的哈希值与 Sender. client 中的值相一致。握手消息(Handshake_messages)中的值包含由客户端问候消息 client hello 开始的，到 Finished 消息为止不包含结束消息在内的所有握手消息，提供给对方检查内容的正确性。

4.4 SSL 记录协议

4.4.1 SSL 记录协议概述

SSL 是层次化协议。在每一层，消息均可以包含描述长度、消息及消息内容的域。SSL 在传输消息时，首先将消息分为可处理的数据块，可以进行压缩，将其封装为一带消息验证(MAC)的包，随后进行加密，并进行传输。收到消息时，首先解密，然后验证、解压缩并重新组合得到原有的消息，将此消息发向高层协议。SSL 记录层从更高层接收未加解释的任意长度的非空块数据块。

4.4.2 打包过程

记录层将数据块分裂为小于或等于 214 字节的 SSLPlainText 记录。客户端消息的分界限并不反映至记录层中，也就是说，具有同样内容类型(ContentType)的多个客户端

消息可能会合并为一个 SSLPlaintext 记录。

4.4.3 记录的压缩和解压缩

所有的记录均应用在当前的对话状态中定义的压缩算法进行压缩。压缩算法初始化定义为 CompressionMethod. null，随后通过用户握手协议协商更改。压缩算法将 SSLPlaintext 结构转换为 SSLCompressed 结构，当 CipherSpec 变换后，压缩函数将删除其状态信息。压缩必须是无损压缩，且对原文长度的增加不超过 1024 比特。如果解压缩函数遇到一待解的超过 214 比特的 SSLCompressed. fragment，它将产生 decompression_failure 报警。

4.4.4 记录保护和加密方法

所有的记录数据均由加密算法和消息验证算法保护。所用的加密算法和消息验证算法定义在加密说明(CipherSpec)和消息验证(MAC)算法中。一般的，CipherSpec 初始化为 SSL_NULL_WITH_NULL_NULL，并不提供任何安全性。只有当握手结束后，双方通过共享秘密加密记录和计算消息验证码(MACs)。进行加密和消息验证(MAC)方法由 CipherSpec 定义，并受 CipherSpec. cipher_type 的限制。加密和消息验证(MAC)函数将 SSLCompressed 结构转换为 SSLCiphertext 结构。解密操作是加密操作的逆过程。记录传输时将包含一序列号，这样当包丢失、被改变或包被重复收到时，可以及时发现。

SSLCiphertex 结构如下：

```
struct
{
    ContentType type;
    ProtocolVersion version;
    uint16 length;
    select (CipherSpec.cipher_type)
    {
        case stream: GenericStreamCipher;
        case block: GenericBlockCipher;
    } fragment;
} SSLCiphertext;
```

其中的参数说明如下。

type：指定为 SSLCompressed. type。

version：指定为 SSLCompressed. version。

length：指明随后的 SSLCiphertext. fragment 长度(单位：字节)。长度不应超过 214+2048。

fragment：包含消息验证码(MAC)的 SSLCompressed. fragment 加密后的形式。

4.5 SSL 密钥更改协议

SSL 密钥更改协议用以通知参与各方加密策略的改变。SSL 密钥更改协议只包含一个使用当前(不是未决的)加密方法(Cipher Spec)加密并压缩过的消息。此消息包含一个字节,其值为1。

ChangeCipherSpec 消息结构如下:

```
struct
{
    enum { change_cipher_spec(1), (255) } type;
} ChangeCipherSpec;
```

更改 Cipher Spec 的消息可以由客户端或服务器发出,通知对方随后的记录将由刚协商好的加密方法(Cipher Spec)和密钥来保护。接收方收到此消息后,将读未决状态(Read Pending State)复制到当前读状态(Read Current State)中。客户端在密钥交换握手和证书验证消息(如果有的话)之后,发出更改加密方法(Cipher Spec)的消息,服务器则在成功处理客户端发来的密钥交换消息后发出一个更改加密方法(Cipher Spec)的消息。意外的更改加密方法(Cipher Spec)消息应产生 Unexpected_message 报警。当重新开始一个原有的对话时,加密方法(Cipher Spec)消息应在问候消息(Hello Messages)之后发出。

4.6 SSL 告警协议

由 SSL 记录层所支持的一种内容类型(Content Types)即为报警类型,报警消息包含报警级别和对报警的描述。最严重一级的报警消息将立即终止连接,在这种情况下,本次会话的其他连接还可以继续进行,但对话标识符失效,以防止此失败的会话重新建立新的连接。与其他消息一样,报警消息是利用由当前连接状态所指定的算法加密和压缩的。

Alert 消息结构如下:

```
struct
{
    AlertLevel level;                    //报警的级别
    AlertDescription description;        //报警的描述
} Alert;
```

4.6.1 关闭报警

客户端和服务器为避免截断攻击,必须共享连接已关闭这一信息,通信双方均可发起

关闭报警信息。通信双方通过发送发起关闭报警(Close_notify Alert),之后的任何数据都将被丢弃。任何一方在关闭处于写状态的连接时,需要发送关闭报警(Close_notify Alert),另一方以立即关闭连接作出响应,丢弃所有挂起的写操作。关闭处于读状态的连接时,不需要等待响应关闭报警。

4.6.2 错误报警

SSL 握手协议中的错误处理相对简单。当发现一个错误后,发现方将向对方发一个消息。当传输或收到严重错误报警消息时,连接双方均立即终止此连接。服务器和客户端均丢弃错误会话使用的标识符、密钥及秘密信息。

SSL 中定义了下列错误报警。

unexpected_message:收到意外的消息,此报警属于严重错误报警,不应在正常的连接中被观察到。

bad_record_mac:当收到带有不正确的 MAC 记录时,将返回此报警。此报警属于严重错误报警。

decompression_failure:解压缩函数收到不合法的输入(如数据太长等),此报警属于严重错误报警。

handshake_failure:收到 handshake_failure 报警消息,表明发出者不能接受现有的选项所提供的安全参数集合,此报警属于严重错误报警。

no_certificate:当被要求给出证书而没有合法的证书时,将发出 no_certificate 报警消息。

bad_certificate:当一证书被破坏或者证书中签名无法被正确认证时,发出此报警。

unsupported_certificate:证书类型不支持。

certificate_revoked:证书被签发者撤销。

certificate_expired:证书过期或失效。

certificate_unknown:未知因素导致的证书不可接受性。

illegal_parameter:握手消息中域值溢出或一致,此报警属于严重错误报警。

4.7 SSL 协议安全性分析

SSL 协议的安全性由采用的加密算法和认证算法所保证。实践证明,现有的加密和认证算法是安全有效的,但随着计算机技术和信息对抗技术的发展,一些新的问题和挑战随即产生。特别值得注意的是,最近以王小云为代表的一群中国密码学家进行的研究表明,MD5 和 SHA-1 并不是无冲突的,而且他们找到了比暴力方式更快找到冲突的算法。这些发现促使产业界不得不发展更安全的散列算法,同时也使开发下一代更安全的 SSL 协议提上了日程。

4.7.1 SSL 协议依赖的加密和认证算法

1. 加密算法和会话密钥

SSL v2.0 协议和 SSL v3.0 协议支持的加密算法包括 RC4、RC2、IDEA 和 DES，而加密算法所用的密钥由消息散列函数 MD5 产生。RC4、RC2 是由 RSA 定义的，其中 RC2 适用于块加密，RC4 适用于流加密。

2. 认证算法

SSL 协议认证算法采用 IEEE x.509 电子证书标准，是通过 RSA 算法进行数字签名来实现的。典型的认证过程包括服务器认证和客户认证。

（1）服务器的认证。服务器方的写密钥和客户方的读密钥、客户方的写密钥和服务器方的读密钥分别是一对私有、公有密钥。对服务器进行认证时，只有用正确的服务器方写密钥加密，ClientHello 消息形成的数字签名才能被客户正确地解密，从而验证服务器的身份。若通信双方不需要新的密钥，则它们各自拥有的密钥已经符合上述条件。若通信双方需要新的密钥，首先服务器方在 ServerHello 消息中的服务器证书中提供了服务器的公有密钥，服务器用其私有密钥，才能正确地解密由客户方使用服务器的公有密钥加密的 MASTER-KEY，从而获得服务器方的读密钥和写密钥。

（2）客户的认证。同上，只有用正确的客户方写密钥加密的内容，才能被服务器方用其读密钥正确地解开。当客户收到服务器方发出的 REQUEST-CERTIFICATE 消息时，客户首先使用 MD5 消息散列函数获得服务器方信息的摘要，服务器方的信息包括 KEY-MATERIAL-0、KEY-MATERIAL-1、KEY-MATERIAL-2、CERTIFICATE-CHALLENAGE-DATA（来自于 REQUEST-CERTIFICATE 消息）、服务器所赋予的证书（来自于 ServerHello）消息。

其中，KEY-MATERIAL-1、KEY-MATERIAL-2 是可选的，与具体的加密算法有关。然后客户使用自己的读密钥加密摘要形成数字签名，从而被服务器认证。

4.7.2 SSL 安全优势

1. 监听和中间人攻击

SSL 使用一个经过通信双方协商确定的加密算法和密钥，对不同的安全级别应用，都可找到不同的加密算法，从而用于数据加密。它的密钥管理处理比较好，每次连接时产生一个密码杂凑函数，生成一个临时使用的会话密钥。除了不同连接使用不同密钥外，在一次连接的两个传输方向上也使用各自的密钥。尽管 SSL 协议为监听者提供了很多明文，但由于采用 RSA 交换密钥具有较好的密钥保护性能，以及频繁更换密钥的特点，因此对监听和中间人式攻击而言，具有较高的防范性。

2. 流量数据分析式攻击

流量数据分析式攻击的核心是通过检查数据包的未加密字段或未加保护的数据包属性来试图攻击。例如,通过检查 IP 包中未加密的 IP 源地址和目标地址,或检测网络流量,攻击者可能知道谁正在参与交互通信,他们在使用何种服务,有时候甚至能得到或推测出一些商业或个人之间的关系。在一般情况下,该攻击是相对无害的,SSL 协议也未试图阻止这种攻击。但是流量数据分析式攻击可能为攻击者提供一些有用信息,在一些特殊情况下,有可能提升攻击成功的概率。

3. 版本重放攻击

当正在执行 SSL v3.0 的通信方执行 SSL v2.0 时,将发生版本重放攻击。SSL v3.0 使用了非随机的 KKC#1 分组类型 2 的消息填充,这有助于使用 SSL v3.0 的服务器检测出版本重放攻击。

4. 检测对握手协议的攻击

攻击者可能试图改变握手协议中的消息,使通信双方选择不同于通常使用的加密算法。这种攻击容易被发现,因为攻击者必须修改一个或多个握手消息。一旦这种情况发生,客户和服务器将计算出不同的 Handshake Message Hashes,这就导致双方不接收彼此发送的 Finished 消息。

5. 会话恢复伪造

当通过恢复一个会话建立一个连接时,将产生新的 MAC Secret 以及加密 Keys。攻击者不可能在不破坏安全 Hash 操作的情况下,通过已知的以前连接的 MAC Secret 或加密 Keys 来获得或破坏新的 Master Secret。所以,如果这个会话的 Master Secret 是安全的,并且 Hash 操作也是安全的,那么新的连接是安全的,且独立于以前的连接。出于安全考虑,建议限制 Session ID 的生存周期,因为获得 Master Secret 的攻击者可能在 Session ID 改变之前假冒受攻击的一方。

6. 短包攻击

短包攻击的基本过程是假设现在的通信是用 DES 加密数据,并用 TCP 传送,那么当传送最后一个报文时,可能明文就只有一个字节,其后就是填充数据。这时,当攻击者截到报文以后,就可用已知的明密文对的另一个加密块去置换这个报文。然后,它可以通过 TCP 校验和是否有效,知道自己截得是否正确。即使不正确,也只不过是使接受方的 TCP 协议认为其出错而丢包,用户不会知道;但如果正确,则可通过接受方发回的 ACK 获知。尽管在这点上看起来 SSL 能被攻击的可能性很小,比如用 SSL 传送 Web 页、URL 请求,但如果客户经常收发一个字节长度的报文,如 TELNET,就需要对这种攻击作较强的防护了。

7. 截取再拼接式攻击

这种攻击方式的大致过程如下：首先,从一些包含敏感数据的包中“切下”一段密文,被

拼接的这段密文是经过仔细选择的，使接收端非常有可能泄露经过解密的明文。SSL v3.0 基本上已经阻止了这种攻击。首先，它对不同的上下文使用了独立的“会话标识符”，这就阻止了“截取再拼接”攻击在不同层次连接之间截获和拼接；其次，SSL v3.0 对所有的加密包使用了较强的认证，在这种防卫之下，“截获再拼接”攻击已基本不易成功。

8. 报文重发式攻击

报文重发式攻击是一种比较容易被阻止的攻击。综上所述，如同防范截取再拼接式攻击一样，SSL 在 MAC 数据中含进序列号，阻止了重放攻击。同时，这种机制也阻止了“延迟”、“重排序”、“删除数据”等攻击方式。

4.7.3 SSL 协议存在的问题

虽然 SSL 在安全性方面已经做得相当完善，但在实际应用中，仍存在着许多安全漏洞。比如基于流量数据分析的攻击，它基于密文长度，能够揭示明文长度，通过检查 IP 包中未加密的 IP 源地址和目标地址，或检测网络流量，攻击者可知道谁正在参与交互通信，他们在使用何种服务，有时候甚至能得到或推测出一些商业或个人之间的关系。除此之外，SSL 协议还存在以下问题。

1. 密钥管理问题

设计一个安全秘密的密钥交换协议是很复杂的，因此，SSL 的握手协议也存在一些密钥管理问题。SSL 的问题表现如下。

（1）客户机和服务器在互相发送自己能够支持的加密算法时，是以明文传送的，存在被攻击修改的可能性。

（2）SSL v3.0 为了兼容以前的版本，可能降低安全性。

所有的会话密钥中都将生成 MASTER-KEY，握手协议的安全完全依赖于对 MASTER-KEY 的保护。因此，在通信中要尽可能少地使用 MASTER-KEY。

2. 加密强度问题

Netscape 依照美国内政部的规定，在它的国际版浏览器及服务器上使用 40 位的密钥。这是因为，依据美国法律，其所使用的 RC4 加密算法对多于 40 位长的加密密钥产品的出口加以限制。而较短的密钥长度意味着较高的破译可能。

Microsoft 公司试图利用一种称为私人通信技术（Private Communication Technology，PCT）的 SSLsuperset 协议来改进现有 SSL 协议的缺点。PCT 会衍生出第二个专门为身份验证用的密钥，这个身份验证算法并不在 RC4 规定的管辖范围。PCT 加入比目前随机数产生器更安全的产生器，因为它也是 SSL 安全链中的一个弱环节。这个随机数产生器提供了产生加密密钥的种子数目（Seed Number）。

3. 数字签名问题

基于 SSL 协议没有数字签名功能，即没有抗否认服务。若要增加数字签名功能，则

需要在协议中打补丁。这样做,在用于加密密钥的同时又用于数字签名,在安全上存在漏洞。PKI体系完善了这种措施,即双密钥机制,将加密密钥和数字签名密钥二者分开,成为双证书机制,从而构成了PKI完整的安全服务体系。

习题4

1. 观察并举例说明日常工作和生活中可能使用SSL安全协议的例子。

2. 调研目前在计算机网络标准化领域具有重要影响力的国际标准化组织,说明目前SSL安全协议标准化进程由谁主导,并思考其原因。

3. SSL协议是分层协议,请简述其各个层次及其功能。

4. 简述SSL协议面临的安全风险。

5. TCP三次握手协议的漏洞,给类似SYN攻击制造了机会,通过发送大量的半连接请求,耗费CPU和内存资源。SSL协议同样也有握手协商过程,是否也会遭受类似攻击?请说明原因。

第 5 章　会话层安全协议

5.1　背景介绍

一些传统的网络服务程序，如 FTP、TELENT、RLOGIN、RSH 和 RCP，在本质上都是不安全的。因为它们在网络上用明文传送口令和数据，别有用心的人非常容易就截获这些口令和数据。而且，这些服务程序的安全验证方式也是有弱点的，就是很容易受到中间人(Man In The Middle)这种方式的攻击。所谓“中间人”的攻击方式，就是“中间人”冒充真正的服务器，接收你传给服务器的数据，然后再冒充你，把数据传给真正的服务器。服务器和你之间的数据传送被“中间人”一转手做了手脚之后，就会出现很严重的问题。以 ARP“中间人”攻击为例，按照 ARP 协议的设计，一个主机收到的 ARP 应答即使并非自身请求得到的，也会将其 IP 地址和 MAC 地址的对应关系添加到自身的 ARP 映射表中。这样可以减少网络上过多的 ARP 数据通信，但也为 ARP 欺骗创造了条件。

如图 5-1 所示，Host A 和 Host C 通过交换机进行通信。此时，如果有黑客(Host B)想探听 Host A 和 Host C 之间的通信，可以分别给这两台主机发送伪造的 ARP 应答报文，使 Host A 和 Host C 用 MAC_B 更新自身 ARP 映射表中与对方 IP 地址相应的表项。此后，Host A 和 Host C 之间看似“直接”的通信，实际上都是通过黑客所在的主机间接进行的，即 Host B 担当了“中间人”的角色，可以对信息进行窃取和篡改。这种攻击方式就称为“中间人(Man In The Middle)攻击”。

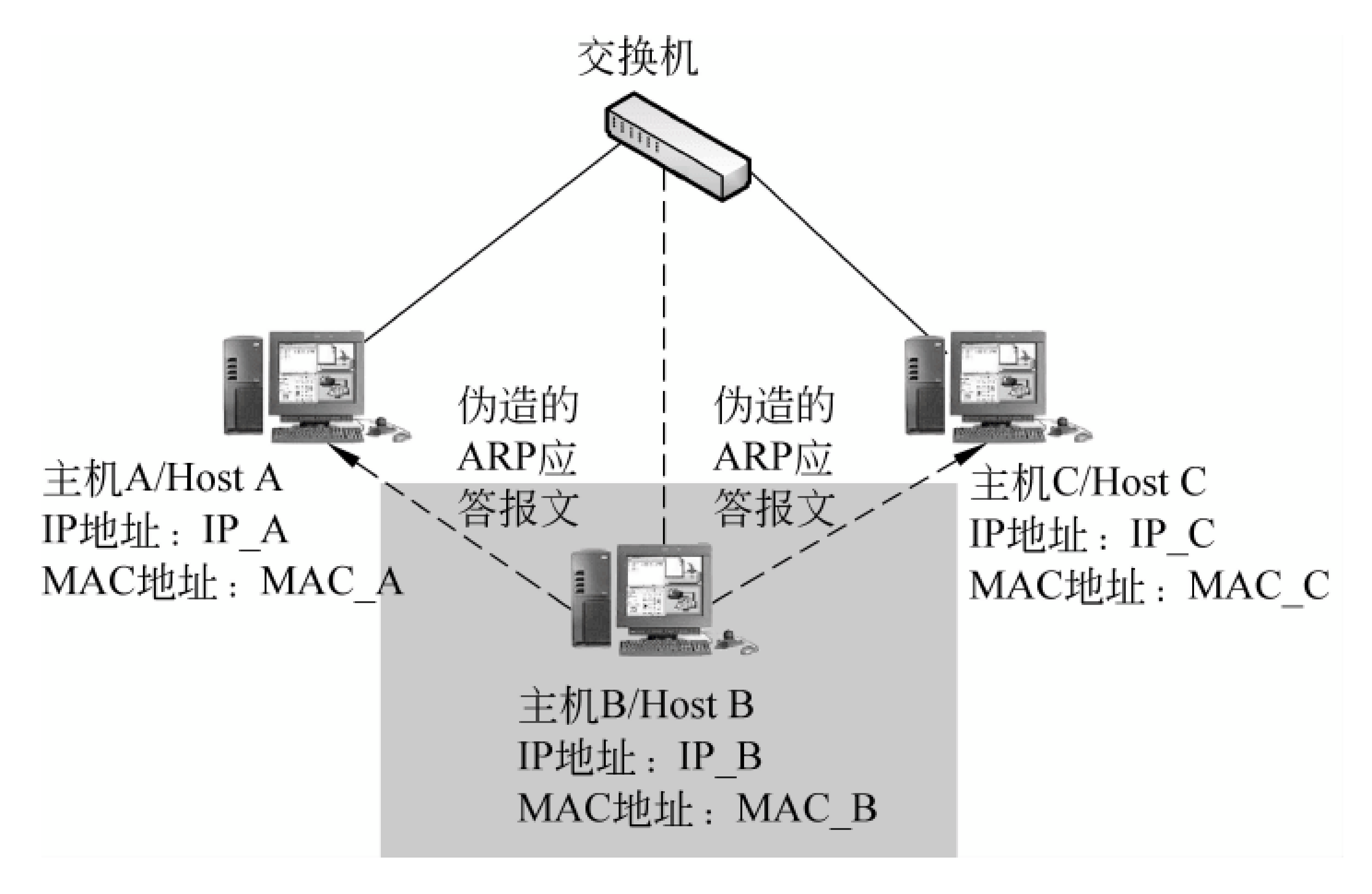


图 5-1　ARP “中间人” 攻击示意图

通过安全外壳协议(Secure Shell Protocol，SSH)可以部分解决这样的问题。SSH 是介于传输层和应用层之间的安全协议(即 OSI 模型中的会话层，图 5-2 显示了 SSH 在协

议栈中的位置），专为远程登录会话和其他网络服务提供安全性协议，通过使用 SSH，可以把所有传输的数据进行加密，这样“中间人”的攻击方式就不可能实现了。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题，防止 DNS 欺骗、IP 欺骗和源路径攻击。使用 SSH，还有一个额外的好处就是传输的数据是经过压缩的，可以加快传输的速度。SSH 有很多功能，它既可以代替 TELNET，又可以为 FTP、POP、甚至 PPP 提供一个安全通道。SSH 使用公共密钥加密法进行用户和主机认证，保护会话的安全。这就比简单地使用密码和主机名进行认证更加安全可靠，包括防止包嗅探，即通过查看你所发数据包的内容获取密码或其他包信息。除了进行认证外，SSH 还提供了加密会话，以防止包欺骗和密码盗用。这就允许用户在一个不安全的网络中使用账号进行数据传输，而所传数据是非明文的。此外，可以使用 POP 通道和 TELNET 方式，通过 SSH，利用 PPP 通道创建一个虚拟专用网络（ Virtual Private Network，VPN ）。

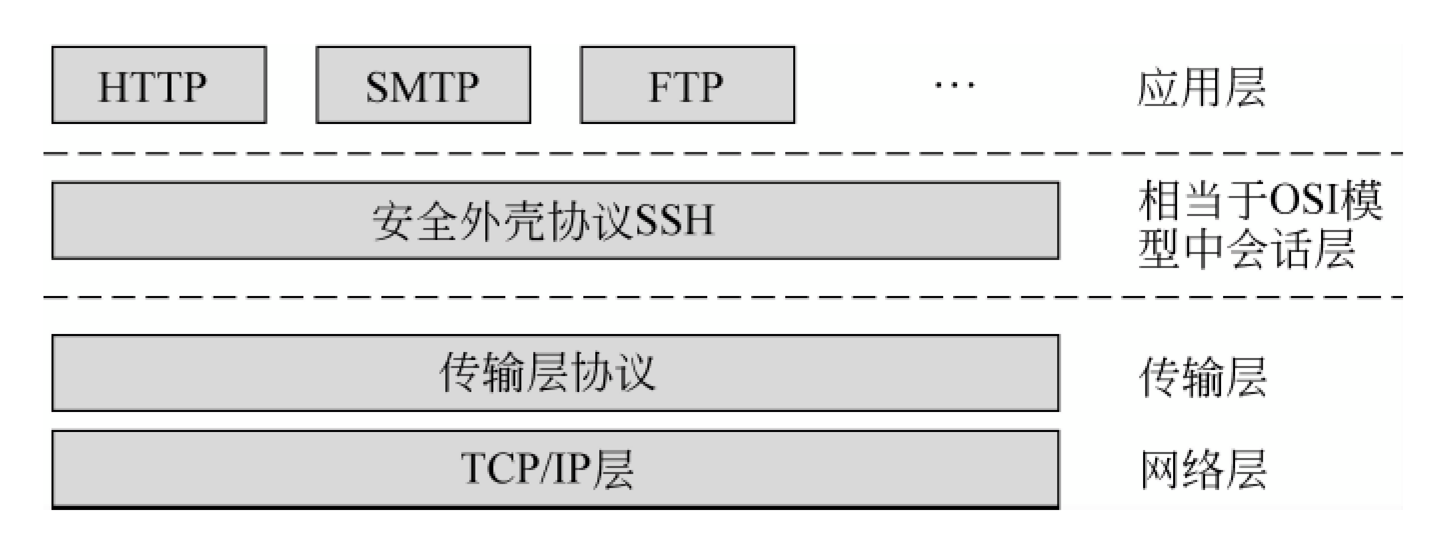


图 5-2　SSH 协议层次结构

在不安全的网络环境中，SSH 通过协议的加密和认证机制，实现了安全的远程访问管理、文件操作等应用。如图 5-3、图 5-4 所示，SSH 客户端既可以通过本地连接，也可以通过广域网连接与 SSH 服务器建立 SSH 通道，实现对 SSH 服务器的访问和控制。

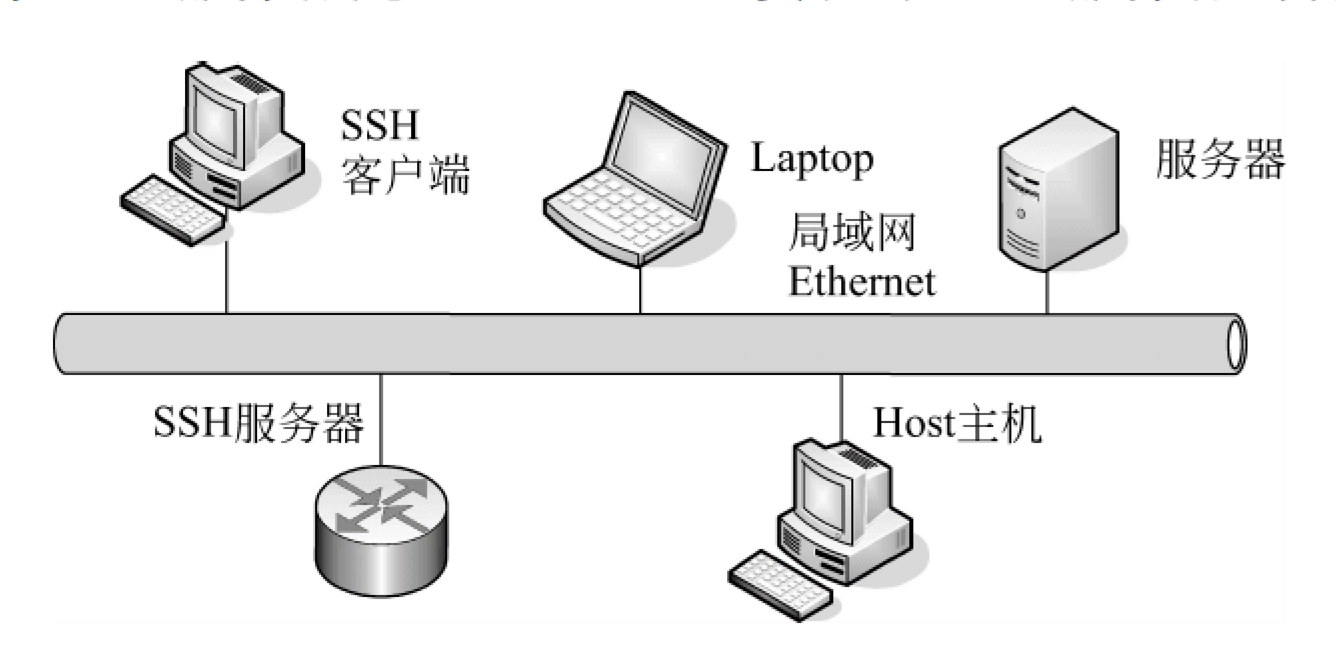


图 5-3　通过本地连接建立 SSH 通道

SSH 最初是 UNIX 系统上的一个程序，后来又迅速扩展到其他操作平台。现行的 SSH 标准由 IETE 的 Secure Shell 工作小组(Secure Shell Group)制定。SSH 易于安装、使用简单，一般的开源系统 UNIX 平台，包括 FreeBSD、HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix、SCO 等都可以运行 SSH。而且在 UNIX 作平台以外，包括 OS/2、VMS、BeOS、Java、Windows 平台，都随系统附带有支持 SSH 的应用程序包。随后，更多的科研单位、大学、公司加入了 SSH 协议的相关研究开发工作，形成了一系列国际标准。

目前流行的 SSH 衍生产品主要有 OpenSSH、Tectia、Putty、Winscp 等。值得注意的

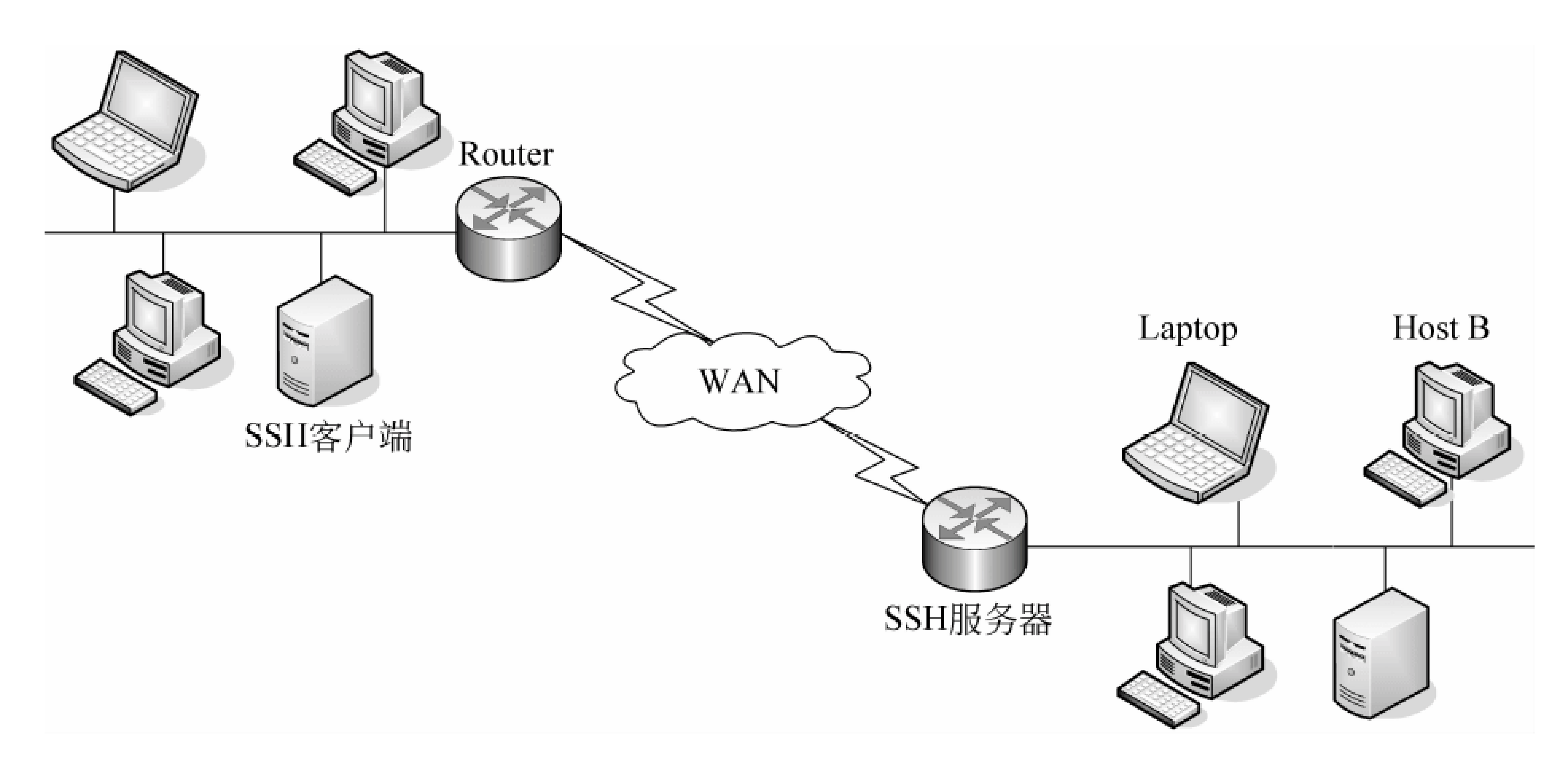


图 5-4　通过广域网连接建立 SSH 通道

是，由于 SSH 受制于版权保护和专利壁垒，以及加密算法的限制，越来越多的用户都转而使用 OpenSSH。OpenSSH 加密所有网络流量，有效消除了第三方窃听、连接劫持和其他潜在攻击。OpenSSH 套件用 SSH、SCP 和 SFTP 代替不安全的 RLOGIN、TELNET、RCP 和 FTP，同时增加了一些新的安全功能组件，包括 sshd、ssh-add、ssh-agent、ssh-keysign、ssh-keyscan、ssh-keygen 和 sftp-server。OpenSSH 支持 Windows、Linux、BSD、Mac、VMS 等平台，这使得 OpenSSH 具有广泛的适用性。OpenSSH 遵守 BSD 许可协议，完全免费和开放源代码，支持用户二次开发。但是 OpenSSH 用于商业用途的时候，使用者应该考虑自己所使用的算法有没有受到本国专利的限制。可以预计，OpenSSL 的使用将会越来越多。

5.2　SSH 协议简介

SSH 协议是一个分层协议，如图 5-5 所示。由三层组成，即传输层协议（Transport Layer Protocol，TLP）、用户认证协议（User Authentication Protocol，UAP）、连接协议（Connection Protocol，CP）。同时，SSH 协议框架还为许多高层的网络安全应用协议提供扩展支持。

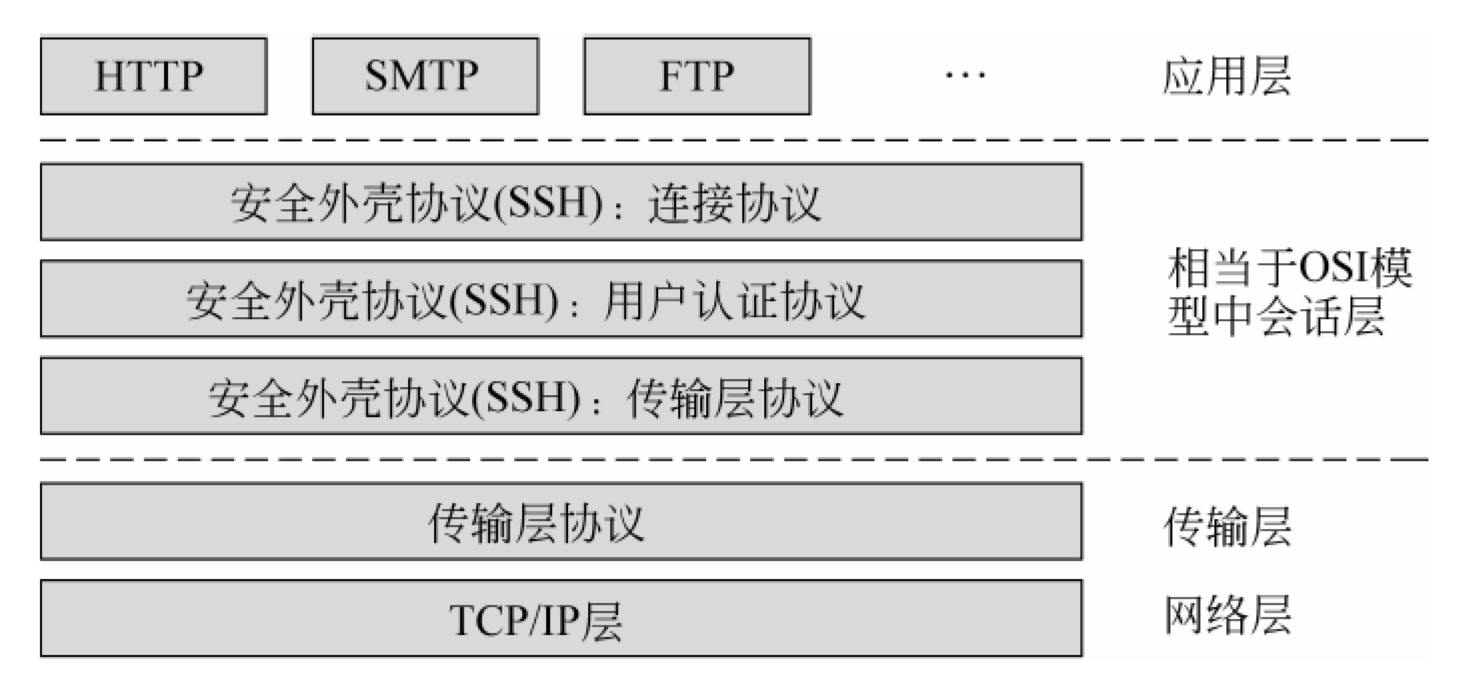


图 5-5　SSH 协议分层结构

(1) 在 SSH 的协议框架中，传输层协议(The Transport Layer Protocol，TTLP)提供服务器身份认证、通信加密、数据完整性校验以及数据压缩等多项安全服务。

(2) 用户认证协议(The User Authentication Protocol，TUAP)则为服务器提供客户端的身份鉴别机制。

(3) 连接协议(The Connection Protocol，TCP)将加密的信息隧道复用成若干个逻辑通道，提供给更高层的应用协议使用；各种高层应用协议可以相对独立于 SSH 基本体系之外，并依靠这个基本框架，通过连接协议使用 SSH 的安全机制。

本书第 5.3 节～第 5.5 节分别介绍 SSH 传输层协议、用户认证协议和连接协议。

5.3 SSH 传输协议

SSH 传输层协议主要在不安全的网络中为上层应用提供一个加密的通信信道。SSH 传输层协议提供服务器身份认证、通信加密、数据完整性校验以及数据压缩等多项安全服务。双方通信所需要的密钥交换方式、公钥密码算法、对称密钥密码算法、消息认证算法和哈希算法等，都可以进行协商。传输层协议通常运行于 TCP/IP 之上，也可以是其他可靠的底层协议。运行 SSH 传输层协议，产生一个会话密钥和一个唯一会话 ID。SSH 传输层协议并不涉及客户端用户的身份认证，传输层产生了口令认证和其他服务需要的(共享)秘密数据。用户认证可以通过基于该协议之上、单独设计的协议来完成。这样既保证了通信的安全性，又提供了协议的灵活性和扩展性。

一般来说，SSH 数据包包含以下内容，如表 5-1 所示。

表 5-1 SSH 数据包内容

类　型	内　　容
uint32	包长 packet_length
byte	填充长度 padding_length
byte[n1]	负载 Payload；n1＝packet_length-padding_length-1
byte[n2]	随机填充 random padding；n2＝padding_length
byte[m]	mac(Message Authentication Code-MAC)；m＝mac_length
packet_length	以字节(byte)计的包长，不包括 mac 与自身(packet_length)域的长度
padding_length	以字节(byte)计的随机填充长度
payload	负载部分，如果协商了压缩算法，本部分将进行压缩。初始化压缩算法为 none
random padding	任意长度的填充，由随机生成的字节构成，最大的填充数量为 255 字节。填充后 packet_length || padding_length || payload || random padding 的总长度应该是密码模块长度或 8 的整数倍
mac	Message Authentication Code。如果进行了认证协商，本部分为计算得到的 MAC 值，初始化 MAC 算法为 none

一般情况下，该协议需要两轮就可以完成密钥交换、服务器认证、客户服务请求和服

务器应答。

首先，双方(使用 SSH 二进制包表示协议格式)相互发送己方支持的算法列表，并按照相同的规则进行匹配。算法列表中包括密钥交换算法、加密算法、MAC 算法、压缩算法等。

随后，双方再进行密钥交换。密钥交换产生两个值：一个共享秘密 K 和一个交换哈希 H。加密和认证的密钥从这两个值中派生出来。作为会话 ID，H 在本次会话中保持不变。该哈希函数同样也用于生成密钥。

SSH 连接的可靠性由底层来保证，所以首先必须保证一个可靠的底层连接。例如，可以基于可靠的 TCP/IP 连接建立的 SSH 连接，此时通常服务器在 22 端口侦听 SSH 连接，这个端口也是 IANA 为 SSH 正式分配的端口号。

SSH 传输层协议主要完成以下几项任务。

5.3.1 版本协商

目前的 SSH 实现中，比较普遍的协议版本号是 SSH 2.0。但是因为还有一些网络设备上运行的是比较老的版本，所以实现时必须考虑版本兼容性问题。

当 TCP 连接建立之后，通信双方都必须向对方发送自己的版本字符串，其中包括 SSH 的协议版本号、软件版本号等，版本字符串的最长是 255 字节。

版本协商包括两种情况：旧版本的客户端和新版本的服务器端之间，以及新版本的客户端和旧版本的服务器端之间。

新版本的服务器端创建时，必须有一个可以配置的兼容选项，来控制是否兼容旧版本的客户端登录。如果兼容，这个服务器端在版本协商阶段往对端发送的协议版本号就是 1.99。如果是 2.0 的客户端登录，1.99 和 2.0 的服务器端对于它来说应该是一致的，而对于 1.5 及以下的客户端来说，1.99 意味着这个服务器兼容 1.5 的版本，版本协商可以通过。如果服务器配置成不兼容 2.0 的协议，那么它向对端发送的协议版本号就是 2.0，当 1.5 的客户端登录时，发现对端的协议版本号是 2.0，版本协商就不会成功，双方断开 TCP/IP 连接。

当新版本的客户端登录旧版本的服务器时，由于客户端不能去兼容服务器，所以遇到旧版本服务器的时候，客户端必须断开连接，使用旧版本再去登录。

版本协商阶段，双方交互的数据都是以明文方式传输的。

5.3.2 算法协商与密钥交换

版本协商成功后，双方就开始采用二进制数据包进行通信。由服务器向客户端发送第一个包，内容为自己的 RSA 主机密钥(Host Key)的公钥部分、RSA 服务密钥(Server Key)的公钥部分、支持的加密方法、支持的认证方法、次协议版本标志以及一个 64 位的随机数(Cookie)。这个包没有加密，以明文方式发送。

表 5-2 算法协商数据包内容

类 型	内 容	类 型	内 容
byte	SSH_MSG_KEXINIT	name-list	mac_algorithms_server_to_client
byte[16]	cookie(random bytes)	name-list	compression_algorithms_client_to_server
name-list	kex_algorithms	name-list	compression_algorithms_server_to_client
name-list	server_host_key_algorithms	name-list	languages_client_to_server
name-list	encryption_algorithms_client_to_server	name-list	languages_server_to_client
name-list	encryption_algorithms_server_to_client	boolean	first_kex_packet_follows
name-list	mac_algorithms_client_to_server	uint32	0(reserved for future extension)

客户端选定各种算法的原则如下：依次从自己支持的算法列表中拿出一种算法，在服务器端发送过来的加密算法中进行匹配，如果匹配成功，这种算法就作为双方协商的算法；如果匹配不成功，客户端再取自己算法列表中的下一个算法进行匹配。如果最后也没有匹配成功，意味着算法协商失败。

算法协商成功后，双方进入密钥交换阶段。密钥交换的目的是生成双方通信的公钥，用于后续数据的加密。这个密钥是经过双方协商产生的，双方中的任意一方都不能单独生成这个密钥。

密钥交换的基本原理如下。

客户端随机选择一个私钥 Xc，$1<Xc<p-1$，计算出式(5-1)。

$$Yc = g\hat{}Xc \bmod p \tag{5-1}$$

将计算出的 Yc 发送给服务器端。其中，p 是一个很大的素数，g 是 p 的素根。p 和 g 是双方共有的一对参数，协议允许双方通过协商获得相同的 p 和 g 参数。

服务器也随机生成一个私钥 Xs，$1<Xs<p-1$，计算出式(5-2)。

$$Ys = g\hat{}Xs \bmod p \tag{5-2}$$

也将计算出的 Ys 发送给客户端。

服务器接收到客户端发送过来的 Yc，按照下面的公式计算出密钥。

$$K = (Yc)\hat{}Xs \bmod p \tag{5-3}$$

客户端接收到服务器端发送过来的 Ys，同样按照下面的公式计算出密钥。

$$K = (Ys)\hat{}Xc \bmod p \tag{5-4}$$

通过上面的方法，客户端和服务器端就可以获得相同的密钥。

由上面分析可以看出，密钥交换算法的安全性建立在计算离散对数的难度之上。算式 $Y=g\hat{}x \bmod p$ 中，由 X 计算 Y 是很容易的，但是要由 Y 计算 X 是非常困难的。在密钥交换算法中，对外公开的只有 p、g、Yc 和 Ys，私钥 Xc 和 Xs 是保密的。其他用户即便获取了 p、g、Yc 和 Ys，也很难推断出私钥 Xc 和 Xs，从而保证了密钥的安全性。

密钥交换算法具有如下优势。

(1) 扩展性更好，不需要网络管理员的多余配置。

(2) 交换得到的密钥保存在内存中，不易被读取和篡改。

(3) 每个连接都会动态生成一次新的密钥，安全性更高。

5.3.3 客户端对服务器端的认证

SSH 协议支持对服务器端进行认证。客户端实现中一般都有一个可选选项,控制客户端首次登录时是否对服务器进行认证。如果设置成首次登录不认证,客户端自动将服务器的公钥保存到本次,如果设置成首次登录认证,服务器发送自己的主机公钥和服务器公钥时,客户端就需要提示用户是否认可对端,由用户完成对服务器合法性的检查,以及决定是否保存对端的公钥。

当客户端以后再次登录的时候,如果本地保存了服务器的公钥,就需要用这个保存的公钥来完成对对端服务器的验证,具体的验证过程如下。

首先,客户端比较对端(服务器端)发送过来的主机公钥与本地保存的主机公钥的模数,如果模数不一致,直接认为对端服务器不合法,退出登录过程,并提示用户。

如果验证两个公钥的模数一致,客户使用服务器的主机公钥,将用于生成会话密钥的 32 字节随机字符串加密发往对端(服务器端)。如果对端是合法的服务器,就能解密出这个 32 字节的随机字符串,并成功生成会话密钥。

从客户端开始发送加密的 32 字节随机字符串开始,双方的通信都是以密文的方式进行的。

5.3.4 数据加密

算法协商阶段成功后,得到了双方进行通信的加密算法和用于加密的密钥。此后,双方交互报文的报文长度字段、填充长度字段、净荷字段、填充字段,都必须使用协商出来的算法加密。双方加密使用密钥的有效长度最少不能低于 128bits,否则无法获得足够的安全性。

双方的加解密过程都是独立进行的,协议规定具体实现必须允许双方加解密方式独立。但是出于实际考虑,协议也建议最好在双方使用相同的加解密算法。

现在常用的加密算法主要有 3des-cbc 和 aes128-cbc。这两种算法是协议规定必须支持或者推荐支持的算法,还有一些其他算法,比如 blowfish-cbc、twofish-cbc、twofish256-cbc,这些算法协议不作强制规定,可以选择支持。

5.3.5 数据压缩

如果通信双方协商了压缩算法,数据包中的负载域(Payload)将用协商的压缩算法进行压缩后传输。packet_length 域和 mac 域的值将从压缩后的负载生成。数据加密在压缩之后进行。

目前,SSH 支持的压缩算法如表 5-3 所示。

zlib 压缩算法定义于 RFC 1950 和 RFC 1951,其他可选的压缩算法定义于 SSH-ARCH 和 SSH-NUMBERS 技术规范中。

表 5-3 SSH 压缩算法类型

名 称	类 型	描 述
none	REQUIRED	no compression
zlib	OPTIONAL	ZLIB(LZ77)compression

5.3.6 数据完整性检查

数据的完整性和真实性是通过在每一个包的结尾部分加入 mac 字段来保证的。mac 字段是通过计算双方的共享密文、包序列号以及数据包的内容得到的。

消息认证算法(mac)和共享密文都是算法协商阶段双方协商得到的。在算法协商阶段之前,是不会用到 mac 字段的,它的长度为 0。算法协商阶段之后,在对数据包进行加密之前完成 mac 字段的计算,计算公式如下:

$$mac = MAC(key, sequence_number \parallel unencrypted_packet) \tag{5-5}$$

其中的 key 就是共享秘密,sequence_number 就是包序列号,unencrypted_packet 是未加密的报文数据,包括长度字段、净荷、填充字段。包序列号是一个由 32 比特表示的数字。第一个包的序列号是 0,以后每次增加 1。这个计数只有当包的个数达到 2^{32} 以后才会清零,中间即使发生了密钥或者算法重协商,不会改变序列号。

一般来说,通信的两个方向的 MAC 算法应该各自独立,不过协议还是建议双方使用相同的 MAC 算法。

目前定义的 MAC 算法有 hmac-sha1、hmac-sha1-96、hmac-md5、hmac-md5-96 和 none。其中第一种算法(hmac-sha1)是必须的,第二种算法(hmac-sha1-96)推荐采用,其他几种算法是可选的,协议不推荐使用 none 这种方式。

目前 SSH 支持的 MAC 算法如表 5-4 所示。

表 5-4 SSH MAC 算法类型

名 称	类 型	描 述
hmac-sha1	REQUIRED	HMAC-SHA1(digest length=key length=20)
hmac-sha1-96	RECOMMENDED	first 96 bits of HMAC-SHA1(digest length=12,key length=20)
hmac-md5	OPTIONAL	HMAC-MD5(digest length=key length=16)
hmac-md5-96	OPTIONAL	first 96 bits of HMAC-MD5(digest length=12,key length=16)
none	OPTIONAL	no MAC;NOT RECOMMENDED

所有以"hmac-*"开头的算法均定义于 RFC2104。"*-n"MACs 表示仅使用结果的前 n 比特。

5.3.7 密钥交换算法

密钥交换算法定义了一次性会话密钥如何产生、如何进行数据的加密和认证以及如

何对服务器进行认证。

协议定义必须支持下面的这种密钥交换算法：diffie-hellman-group1-sha1 和 diffie-hellman-group14-sha1。

通过 diffie-hellman 交换算法可以产生一个共享的密钥，这个密钥由双方共同决定，而不是由其中任意一方决定的。密钥交互算法的安全性在于计算离散对数的难度，密钥交换算法后面一般都带有一个对服务器进行认证的数字签名。

5.3.8 主机公钥算法

SSH 协议被设计成可以使用任何格式、编码方式、加密与/或数字签名算法的公钥。公钥类型主要包括以下 4 个方面。

（1）密钥格式，主要是定义密钥怎么编码，以及公钥模数如何表示。

（2）数字签名与加密算法，一些密钥可能不会同时支持加密和数字签名。

（3）对数字签名与加密字段的编码格式。

（4）协议目前定义了几种公钥算法，其中必须支持的是 ssh-dss，推荐支持 ssh-rsa。

几种公钥算法如表 5-5 所示。

表 5-5　SSH 公钥算法类型

名　称	类　型	描　述
ssh-dss	REQUIRED	sign　Raw DSS Key
ssh-rsa	RECOMMENDED	sign　Raw RSA Key
pgp-sign-rsa	OPTIONAL	sign　OpenPGP certificates(RSA key)
pgp-sign-dss	OPTIONAL	sign　OpenPGP certificates(DSS key)

其他的密钥类型定义于 SSH-ARCH 和 SSH-NUMBERS 技术规范中。

5.3.9 密钥重交换

通信的任何一端都可以发起密钥重交换，但是角色不能发生改变，即服务器仍然还是服务器，客户端仍然还是客户端。发起一方首先发送 SSH_MSG_KEXINIT 消息到对端，接收端收到这条消息之后，也回复一个 SSH_MSG_KEXINIT 消息。

密钥重交换与最开始时候的密钥交换基本一致，只是密钥重交换不会改变会话 ID。在密钥重交换阶段，允许改变部分或全部算法，主机密钥也可以改变，压缩和加密用的密文也能重设。

协议建议当双方交互的数据达到吉字节(gigabyte，GB)，或者双方通信的时间达到一个小时，就进行一次密钥重交换。但是由于密钥重交换涉及到公钥操作，这个操作相当占用系统资源，所以重交换也不能过于频繁。

5.4 SSH身份认证协议

SSH用户认证协议提供服务器对用户的认证。SSH用户认证协议使用传输协议提供的会话ID,并依赖传输协议提供的完整性和机密性保证。SSH用户认证协议主要包括以下几种用户认证方式：公钥认证方式、口令认证方式和基于主机的认证方式。在三种用户认证方式中,基于口令的用户认证协议运用最为广泛,大多数用户没有自己的公钥和私钥,而是通过用户名和口令登录服务器。用户的口令既可以是静态口令,也可以动态生成。

5.4.1 公钥认证方式

SSH协议唯一要求必须实现的认证方式就是基于公钥的认证。在这种方式中,用户用私钥来表明自己的身份。简单地说,就是用户向服务器发送一个用自己私钥签名的数据,服务器首先检查该用户的私钥是否可以作为一个有效的认证凭证(通过检查本地数据库中是否存有与之对应的公钥),然后检查该签名的有效性,如果两个条件都满足,用户的认证请求就可以被接受,否则拒绝。

协议使用publickey来标识这种认证方式,所有应用都必须支持这种认证方式。但不是所有的用户都必须使用公钥,很多服务器配置成允许用户不使用这种认证方式。

客户端创建自己的密钥对(公钥/私钥)后,将公钥提前保存到服务器端,私钥在本地以密文的方式进行保存。用户登录时,使用自己的私钥向服务器证明自己的合法性身份。具体的认证过程如下。

首先,客户端发送SSH_MSG_USERAUTH_REQUEST消息到服务器端,认证请求的类型是none,获得服务器端要求的认证方式列表。这里假设服务器只要求用户进行公钥认证,服务器向客户端发起认证挑战中的认证方式列表中就只有publickey一种。

收到认证挑战后,客户端开始进行publickey认证尝试,向服务器端发送以下消息。

```
byte       SSH_MSG_USERAUTH_REQUEST
string     User
string     service
string     "publickey"
boolean    FALSE
string     Public
string     Public
```

服务器收到这条消息后,首先对密钥的合法性进行检查,一般检查密钥的一些验证信息,比如模数等。如果检查通过,就会返回下面这条消息。

```
byte       SSH_MSG_USERAUTH_PK_OK
string     public key algorithm name from the request
string     public key blob from the request
```

以上这个交互过程只是完成了对密钥合法性的检查，真正意义上的用户身份认证过程随后展开。

客户端使用用户自己的私钥生成一个数字签名，并发往服务器端，内容如下。

```
byte      SSH_MSG_USERAUTH_REQUEST
string    User
string    service
string    "publickey"
boolean   TRUE
string    Public
string    Public
string    signature
```

这个数字签名是用户使用自己的私钥，对以下这些数据，通过某种数字签名算法运算得到的。

```
string   session identifier
byte     SSH_MSG_USERAUTH_REQUEST
string   user name
string   service name
string   "publickey"
booean   TRUE
string   public key algorithm name
string   public key to be used for authentication
```

服务器接收到这条消息后，首先检查是否支持对提供的公钥进行认证，如果支持，服务器就开始对数字签名进行检查。

检查过程是这样的，服务器使用自己本地保存的该用户的公钥，按照某种数字签名的算法得到一个结果，按照上面的信息格式检查结果是否正确，如果正确，数字签名就通过。

如果上述两项检查都通过，这种认证方式就通过了，否则，服务器拒绝。当然，即使通过了 publickey 认证，服务器如果还要求其他方式的认证，还会向客户端发起认证挑战。

5.4.2 口令认证方式

所有的应用都应该支持口令认证方式。在此过程中，客户机和服务器都应该检验传输层所提供的机密性。如果没有提供加密，口令认证不能完成；如果没有机密性或 MAC 保障，则不能改变口令。

这种认证方式的标识是"password"，所有的实现都应该支持这种认证方式，这种类型认证的消息包格式如下：

```
byte      SSH_MSG_USERAUTH_REQUEST
string    user name
string    service name
string    "password"
```

```
boolean   FALSE
string    plaintext password in ISO-10646 UTF-8 encoding [RFC3629]
```

在这个消息包中，密码是明文形式的，但是整个包是必须经过 SSH 传输层加密的，所以最终来说，密码是以密文方式传输的。正是因为如此，如果传输层不提供对数据机密性的保证，密码认证这种方式必须被废弃，否则用户的信息无法保证安全。同样，如果传输层不提供机密性的保证，修改密码也应该被禁止。

一般来说，服务器会回应客户端认证成功或者失败的消息。

如果该用户只需要进行密码认证，认证成功发送 SSH_MSG_USERAUTH_SUCCESS。

如果该用户还需要进行其他方式的认证(比如公钥认证)，密码认证成功后，服务器发送 SSH_MSG_USERAUTH_FAILURE 消息给客户端，其中携带需要继续进行的认证方式的列表。

如果密码认证失败，服务发送 SSH_MSG_USERAUTH_FAILURE 消息给客户端。

如果密码过期，服务器需要发送 SSH_MSG_USERAUTH_PASSWD_CHANGEREQ 消息到客户端。服务器不允许用户使用一个已经过期的公钥完成认证。

客户端可以继续尝试使用其他的认证方式，也可以要求用户使用新的密码进行认证。若是后者，可以通过向服务器发送一条 SSH_MSG_USERAUTH_REQUEST 消息，在这条消息中携带旧的密码和用户的新密码，服务器可以依照实际情况，按照下面四种方式进行回复。

回复 SSH_MSG_USERAUTH_SUCCESS 消息，密码被成功修改，并且认证已经成功通过。

回复 SSH_MSG_USERAUTH_FAILURE 消息，并且是部分通过认证，表明密码已经修改成功，但是还要继续进行其他方式的认证。

回复 SSH_MSG_USERAUTH_FAILURE，但是没有注明部分认证通过，表明密码并没有被修改，或者是不允许进行密码修改，或者是旧的密码不对。需要注意的是，如果服务器已经发送 SSH_MSG_USERAUTH_PASSWD_CHANGEREQ 消息，说明服务器是支持密码修改的。

回复 SSH_MSG_USERAUTH_CHANGEREQ，密码修改没有成功，因为新的密码不符合要求(长度太短或是复杂度不够)。

5.4.3 基于主机的认证方式

本方式根据用户来自的主机及远端主机上的用户名来认证。这种认证方式是以 hostbased 来标识的。部分站点希望可以提供基于用户所在主机以及主机名称的认证。这种认证方式不适合于需要高安全性的场所，但是使用非常方便。

这种认证方式是可选的。如果采用这种方式进行认证，需要采取措施，防止一般用户获取主机的公钥。

客户端通过发送以下消息发起基于主机的认证，类似 Linux 系统上的 rhosts 命令。

```
byte      SSH_MSG_USERAUTH_REQUEST
```

```
string    user name
string    service name
string    "hostbased"
string    public key algorithm for host key
string    public host key and certificates for client host
string    client host name expressed as the FQDN in US-ASCII
string    user name on the client host in ISO- 10646 UTF-8 encoding [RFC3629]
string    signature
```

这里的数字签名，是使用用户主机的私钥对下面这些数据进行数字签名得到的，数据的格式如下：

```
string    session identifier
byte      SSH_MSG_USERAUTH_REQUEST
string    user name
string    service name
string    "hostbased"
string    public key algorithm for host key
string    public host key and certificates for client host
string    client host name expressed as the FQDN in US-ASCII
string    user name on the client host in ISO-10646 UTF-8 encoding [RFC3629]
```

服务器必须验证公钥，判断是否真的属于消息包中用户所在的主机，还要使用相应的公钥验证数字签名的合法性。

如果服务器只要求该用户进行基于主机名的认证，用户名就没有意义了，可以被忽略掉。如有可能，还是建议服务器进行一些其他检查，比如检查对端的 IP 地址与用户所在的服务器 IP 地址匹配，这样可以使对主机公钥的安全性依赖更小一些。但是这样的检查对于穿越防火墙的应用就比较麻烦了。

这一层协议的主要作用是提供服务器对登录用户的验证，限制非授权用户的访问。它必须运行在一个安全的传输层协议之上。传输层必须已经完成了对服务器的合法性检查，并已经经过协商，获得了一个加密的数据通道，双方已经经过计算，得到一个会话 ID。总之，需要传输层协议为后续的密码认证和其他认证方式提供一个安全性保障。

当然，除了以上提到的几种认证方式之外，SSH 协议中还规定了一些其他认证方式。这些认证方式满足特定需求，比如上面提到的“None 认证方式”。None 方式比较特殊，服务器不支持这种认证方式，但是对于客户端而言，发送这种认证方式的认证请求，可以获得服务器端支持的认证方式列表。客户端发送“none”的认证请求给服务器，服务器如果支持，就发送 SSH_MSG_USERAUTH_SUCCESS，认证通过；如果不支持，就通过消息 SSH_MSG_USERAUTH_FAILURE，告诉客户端自己支持的认证方式列表。

5.5 SSH 连接协议

SSH 连接层协议的主要功能是完成用户请求的各种具体网络服务，而这些服务的安全性是由底层的 SSH 传输层协议和用户认证层协议实现的。在 SSH 用户成功认证后，

多个信道通过复用到两个系统间的单个连接上而打开。每个信道处理不同的终端会话。客户可以基于服务器建立新的信道,每个信道在每一端被编排给不同的号码。在一方试图打开一个新的信道时,该信道在该端的号码随请求一起传送,并被对方存储,用于指示特定类型业务的通信给该信道。这样使不同类型的会话不会彼此影响,而关闭信道时,也不会影响系统间建立的初始 SSH 连接。利用连接层协议提供的信道,用户可以方便地扩展更广范围的应用。标准方法提供了安全的交互式 Shell 会话、任意 TCP/IP(Tunneling)端口和 X11 连接转发等。

这层协议的服务类型是 ssh-connection。

5.5.1 通道机制

所有的终端会话以及前向连接都是一个通道。

一个连接上可以有多个通道,并以通道 ID 区分。通信双方都使用一个通道 ID 来标示通道号(但是双方记录的通道 ID 有可能不一样)。通道建立请求报文中携带了发送方的通道 ID,其他通道相关的消息中携带的是接收方的通道 ID。

1. 打开通道

通信双方的任何一方想打开通道,都需要在本地获得一个通道 ID。接下来向对端发送以下这条消息:

```
byte      SSH_MSG_CHANNEL_OPEN
string    channel type in US-ASCII only
uint32    sender channel
uint32    initial window size
uint32    maximum packet size channel type specific data follows
```

其中,channel type 是通道类型名称,sender channel 是发送方本地的通道 ID,initial window size 告诉对端可以向本端发送多少字节的数据而不必调整窗口,maximum packet size 告诉对端一次发送的最大包长度。有些应用需要包延时比较小,以获得较好的交互效果,这时就需要把 maximum packet size 设计得尽量小一些。

对端确认自己这端能否打开通道,如果能打开,则回应对端如下的确认消息:

```
byte      SSH_MSG_CHANNEL_OPEN_CONFIRMATION
uint32    recipient channel
uint32    sender channel
uint32    initial window size
uint32    maximum packet size channel type specific data follows
```

其中,recipient channel 就是通道打开请求消息中注明的通道 ID,而 sender channel 就是对端自己分配的通道 ID。

如果不能打开,比如 SSH_MSG_CHANNEL_OPEN 消息的接收端不支持消息中指定的通道类型(channel type),则回应如下的失败消息:

```
byte      SSH_MSG_CHANNEL_OPEN_FAILURE
uint32    recipient channel
uint32    reason code
string    description in ISO-10646 UTF-8 encoding [RFC3629]
string    language tag [RFC3066]
```

客户端可以将 description 中的内容显示给用户，消息中 reason code 的主要取值如表 5-6 所示。

表 5-6　reason code 类型

Symbolic name	reason code
SSH_OPEN_ADMINISTRATIVELY_PROHIBITED	1
SSH_OPEN_CONNECT_FAILED	2
SSH_OPEN_UNKNOWN_CHANNEL_TYPE	3
SSH_OPEN_RESOURCE_SHORTAGE	4

2. 窗口大小的调整

上面的 SSH_MSG_CHANNEL_OPEN 消息中的窗口大小确定了最大可以发送多少数据，而不至于进行窗口大小调整。

双方都可以发送下面这条消息来调整窗口大小：

```
byte      SSH_MSG_CHANNEL_WINDOW_ADJUST
uint32    recipient channel
uint32    bytes to add
```

收到这条消息后，接收方可以增加消息中指定的字节数，这也意味着对端的窗口变大了。实际应用中，窗口的大小最大可以增加到 $2^{32}-1$ 字节。

3. 数据传输

数据是以下面这种格式进行传输的：

```
byte      SSH_MSG_CHANNEL_DATA
uint32    recipient channel
string    Data
```

数据包的最大长度是取对端允许的最大包长度、对端窗口大小中的较小值。

窗口大小随着数据包的发送逐次递减。

可能一些应用在传输层做了最大包长的限制(但是这种限制都必须大于 32768 字节)。这种情况下，连接层对发送包长度也要作一定限制，以免底层传输层截包，造成数据传输的不连续。

此外，一些通道上能够传输好几种类型的数据流。比如，交互会话中有一种 stderr 数据，可以通过 SSH_MSG_CHANNEL_EXTENDED_DATA 这种消息格式来传输，内容如下：

```
byte      SSH_MSG_CHANNEL_EXTENDED_DATA
uint32    recipient channel
uint32    data_type_code
string    Data
```

这里的 data_type_code 定义依赖于各种不同类型的 channel 类型。目前为止，只定义了如下这种通道类型，如表 5-7 所示。

表 5-7 data_type_code 类型

Symbolic name	reason code
SSH_EXTENDED_DATA_STDERR	1

4. 关闭通道

如果一方不再使用该通道进行数据传输，应该关闭通道，此时发送 SSH_MSG_CHANNEL_EOF 消息，内容如下：

```
byte     SSH_MSG_CHANNEL_EOF
uint32   recipient channel
```

发送这条消息不占用窗口大小，甚至在对端窗口为空时，这条消息仍然可以发送。收到这条消息后，不需要进行回复。需要注意的是，通道仍然是开启的，通道的另一个方向仍然能够正常发送数据。如果一方确实需要关闭通道，它需要发送 SSH_MSG_CHANNEL_CLOSE 消息。对端收到这条消息之后，必须也回复一条这个消息，除非这端已经发送过这条消息。当双方都已经发送，并已经收到 SSH_MSG_CHANNEL_CLOSE 后，就可以认为通道已经关闭了。通道关闭后，通道 ID 可以回收，内容如下：

```
byte     SSH_MSG_CHANNEL_CLOSE
uint32   recipient channel
```

用户可以在未发送 SSH_MSG_CHANNEL_EOF 的情况下发送 SSH_MSG_CHANNEL_CLOSE。但协议建议，如果有可能，最好等所有数据都达到对端后再发送这条消息。

5. 通道类型信息的请求

许多通道类型还有一些关于这个通道类型的扩展说明。例如，可以在交互会话中申请一个虚拟终端(PTY)，通过通道类型信息请求获取这些说明。

所有通道类型信息请求都采用下面这种消息格式，内容如下：

```
byte      SSH_MSG_CHANNEL_REQUEST
uint32    recipient channel
string    request type in US-ASCII characters only
boolean   want reply type-specific data follows
```

如果 want reply 这一位是 False，就不要对这条消息进行回复，如果是 True，就必须对这条消息进行回复，可以回复以下三种消息中的一种，内容如下：

```
SSH_MSG_CHANNEL_SUCCESS
SSH_MSG_CHANNEL_FAILURE
request-specific continuation messages
```

如果接收端不支持这种通道类型信息的请求，就要发送 SSH_MSG_CHANNEL_FAILURE 消息。与上面的 SSH_MSG_CHANNEL_EOF 消息一样，这条消息不占用发送对端窗口大小，即使对端窗口大小为 0，这条消息也仍然能够发送成功。同样，回复的信息也不占用通道窗口大小。request type 是与通道类型相关的，各个通道类型都可以定义自己的 request type。

客户端可以在接收到对端对这条请求信息的回复之前继续发送一些相关的信息。

5.5.2 交互会话

会话就是程序的远程执行，这个程序可能是一个 Shell、应用、系统命令或者内嵌的子系统。

1. 开始会话

会话的开始是通过发送下面这条消息进行的。

```
byte     SSH_MSG_CHANNEL_OPEN
string   "session"
uint32   sender channel
uint32   initial window size
uint32   maximum packet size
```

具体实现中，SSH 的客户端应该拒绝任何会话通道打开的请求，以防止一些恶意服务器攻击客户端。

2. 请求建立一个虚拟的终端(Pseudo-Terminal)

通过发送下面这条消息，为一个会话过程建立一个虚拟终端。

```
byte      SSH_MSG_CHANNEL_REQUEST
uint32    recipient channel
string    "pty-req"
boolean   want_reply
string    TERM environment variable value(e.g.,vt100)
uint32    terminal width,characters(e.g.,80)
uint32    terminal height,rows(e.g.,24)
uint32    terminal width,pixels(e.g.,640)
uint32    terminal height,pixels(e.g.,480)
string    encoded terminal modes
```

主要定义终端显示的一些参数，其中 pixels 定义可以用于显示的窗口大小，而

characters/rows 定义实际显示的窗口大小。

客户端可以忽略建立虚拟终端 pty 的请求。

3. X11 转发

X11 转发通过会话发送 SSH_MSG_CHANNEL_REQUEST 消息发出请求，消息格式如下：

```
byte      SSH_MSG_CHANNEL_REQUEST
uint32    recipient channel
string    x11-req
boolean   want reply
boolean   single connection
string    x11 authentication protocol
string    x11 authentication cookie
uint32    x11 screen number
```

当会话信道关闭时，X11 连接转发立即结束，但是已经开启的转发不会自动关闭。X11 信道响应信道开启请求 SSH_MSG_CHANNEL_OPEN 而打开，信道独立于会话，关闭会话不会关闭 X11 转发信道。消息格式如下：

```
byte     SSH_MSG_CHANNEL_OPEN
string   x11
uint32   sender channel
uint32   initial window size
uint32   maximum packet size
string   originator address(e.g.,"192.168.7.38")
uint32   originator port
```

接收方以 SSH_MSG_CHANNEL_OPEN_CONFIRMATION 消息或 SSH_MSG_CHANNEL_OPEN_FAILURE 消息响应信道开启成功或失败。

4. 环境变量传递

环境变量可以传递给即将开启的 Shell/Command。在特权进程中，不受控制的环境变量设置可能成为安全隐患。建议维护一个允许的变量列表，或直至服务进程权限降低后才进行环境变量设置。SSH_MSG_CHANNEL_REQUEST 消息格式如下：

```
byte      SSH_MSG_CHANNEL_REQUEST
uint32    recipient channel
string    Env
boolean   want reply
string    variable name
string    variable value
```

5. 开启 shell/command

一旦通话建立起来后，在远端的程序就开始执行了。这个程序可以是一个 Shell，也可以是一个应用程序，或者是拥有主机独立名字的一个子系统。

(1) 开启远端 shell/。

开启远端 shell 的消息格式如下：

```
byte       SSH_MSG_CHANNEL_REQUEST
uint32     recipient channel
string     Shell
boolean    want reply
```

这条消息用于在远端开始执行用户默认的 Shell(UNIX 系统下是在/etc/passwd 目录下)。

(2) 开启远端 command。

开启远端 command 的消息格式如下：

```
byte       SSH_MSG_CHANNEL_REQUEST
uint32     recipient channel
string     Exec
boolean    want reply
```

这条消息用于在服务器上执行指定的命令。由于系统命令是有权限划分的，这里必须对命令的执行进行权限的控制，否则会引起非授权命令执行的情况发生。

(3) 开启远端子系统(subsystem)。

开启远端子系统(subsystem)command 的消息格式如下：

```
byte       SSH_MSG_CHANNEL_REQUEST
uint32     recipient channel
string     subsystem
boolean    want reply
string     subsystem name
```

这个消息用于服务器端启动一个预先定义好的子系统，这个子系统应该包括一个通用的文件传输机制，还有一些其他特性，并允许更多的配置机制。

6. 会话数据的传输

会话数据通过 SSH_MSG_CHANNEL_DATA 及 SSH_MSG_CHANNEL_EXTENDED_DATA 消息传输。stderr data 已经定义了 SSH_EXTENDED_DATA_STDERR 这种数据类型。

7. 窗口尺寸更改消息(Window Dimension Change Message)

当客户终端窗口尺寸更改时，将会发送以下消息给对端。消息格式如下：

```
byte      SSH_MSG_CHANNEL_REQUEST
uint32    recipient channel
string    window-change
boolean   FALSE
uint32    terminal width,columns
uint32    terminal height,rows
uint32    terminal width,pixels
uint32    terminal height,pixels
```

8. 本地流量控制 Local Flow Control

许多系统能够判断虚拟终端是否使用 control-S/control-Q 流量控制。客户端流量能够加速对用户请求的响应。服务器端发送以下消息，通知客户端是否执行流量控制，消息格式如下：

```
byte      SSH_MSG_CHANNEL_REQUEST
uint32    recipient channel
string    xon-xoff
boolean   FALSE
boolean   client can do
```

如果 client can do 域为 True，客户端使用 control-S 和 control-Q 进行流量控制。

9. 信号 Signals

通过以下消息，信号能够被传送给远端进程/服务。对于不支持信号的子系统，将忽略本消息。消息格式如下：

```
byte      SSH_MSG_CHANNEL_REQUEST
uint32    recipient channel
string    Signal
boolean   FALSE
string    signal name(without the"SIG"prefix)
```

10. 返回退出状态

当命令运行在其他终端时，以下消息能够返回命令的退出状态，消息格式如下：

```
byte      SSH_MSG_CHANNEL_REQUEST
uint32    recipient channel
string    exit-status
boolean   FALSE
uint32    exit_status
```

远端命令也可以通过信号暴力中断，这种情况下传送的消息格式如下：

```
byte      SSH_MSG_CHANNEL_REQUEST
```

```
uint32    recipient channel
string    exit-signal
boolean   FALSE
string    signal name(without the"SIG"prefix)
boolean   core dumped
string    error message in ISO-10646 UTF-8 encoding
string    language tag [RFC3066]
```

信号名可能取值为 ABRT、ALRM、FPE、HUP、ILL、INT、KILL、PIPE、QUIT、SEGV、TERM、USR1 和 USR2。

5.6 SSH 应用

SSH 协议被设计成一种通用的安全协议，它不仅能应用为安全的 Telnet，还有一些其他安全性方面的应用，比如 SSH2.0 协议内置的 SFTP 功能等。此外 SSH 还有另一项非常有用的功能，就是它的端口转发隧道功能。此功能让一些不安全的服务，如 POP3、SMTP、FTP、LDAP 等通过 SSH 的加密隧道传输，使得原本不安全的明文传输方式经过加密通道后，变成了安全的密文方式，中间媒介不能轻易地监听到协议传输的数据。SSH 的“加密通道”是通过“端口转发”来实现的。用户可以在本地端口(没有用到的)和远程服务器上运行的某个服务端口之间建立“加密通道”，然后只要连接到本地端口即可。所有对本地端口的请求都被 SSH 加密，并且转发到远程服务器的端口。当然，只有远程服务器上运行 SSH 服务器软件的时候，“加密通道”才能工作。端口转发(Port Forward)有两种，即本地端口转发(Local Forward)和远端端口转发(Remote Forward)。

接下来，我们将给出利用 SSH 本地端口转发功能构建安全 VPN 的实例。

移动银行服务是无线通信技术与银行业务相结合的产物。它将无线通信技术的 3A 优势应用到金融业务中，为客户提供在线、实时的服务。例如，银行需要上门为一些大型企业的职工或客户现场发行储蓄卡，从而要求将银行的柜面系统从营业网点搬到客户处。同时，由于上门办理业务具有临时性、流动性特点，无法租用固定专线联网，考虑到成本和现有通信条件，只能使用无线通信方式联网。在这样的环境下，如何保障信息和数据的安全，成为迫切需要解决的问题。图 5-6 展示了基于 SSH 协议实现的银行无线移动柜台。

无线移动柜台前台硬件设备是一台装有无线网卡的笔记本计算机，一台网络终端通过以太网卡和一根直连双绞线连接到笔记本计算机上，网络终端接有读卡器和便携式票据打印机，可以刷卡、打印凭证。笔记本计算机安装 Windows 2000 系统，并安装运行 OpenSSH for Windows 客户端软件。笔记本计算机通过无线上网，笔记本计算机上运行 OpenSSH for Windows 客户端程序，事先生成的密钥经过安全认证，通过因特网连接到银行机房的后台 OpenSSH 服务端，并获得一个通信加密密钥。然后按照配置的端口监听并接收来自网络终端的登录请求，用通信加密密钥加密后送往后台 OpenSSH 服务端。后台设备，即 SSH 安全认证服务器安放在中心机房。系统内置安装了 OpenSSH 服务端

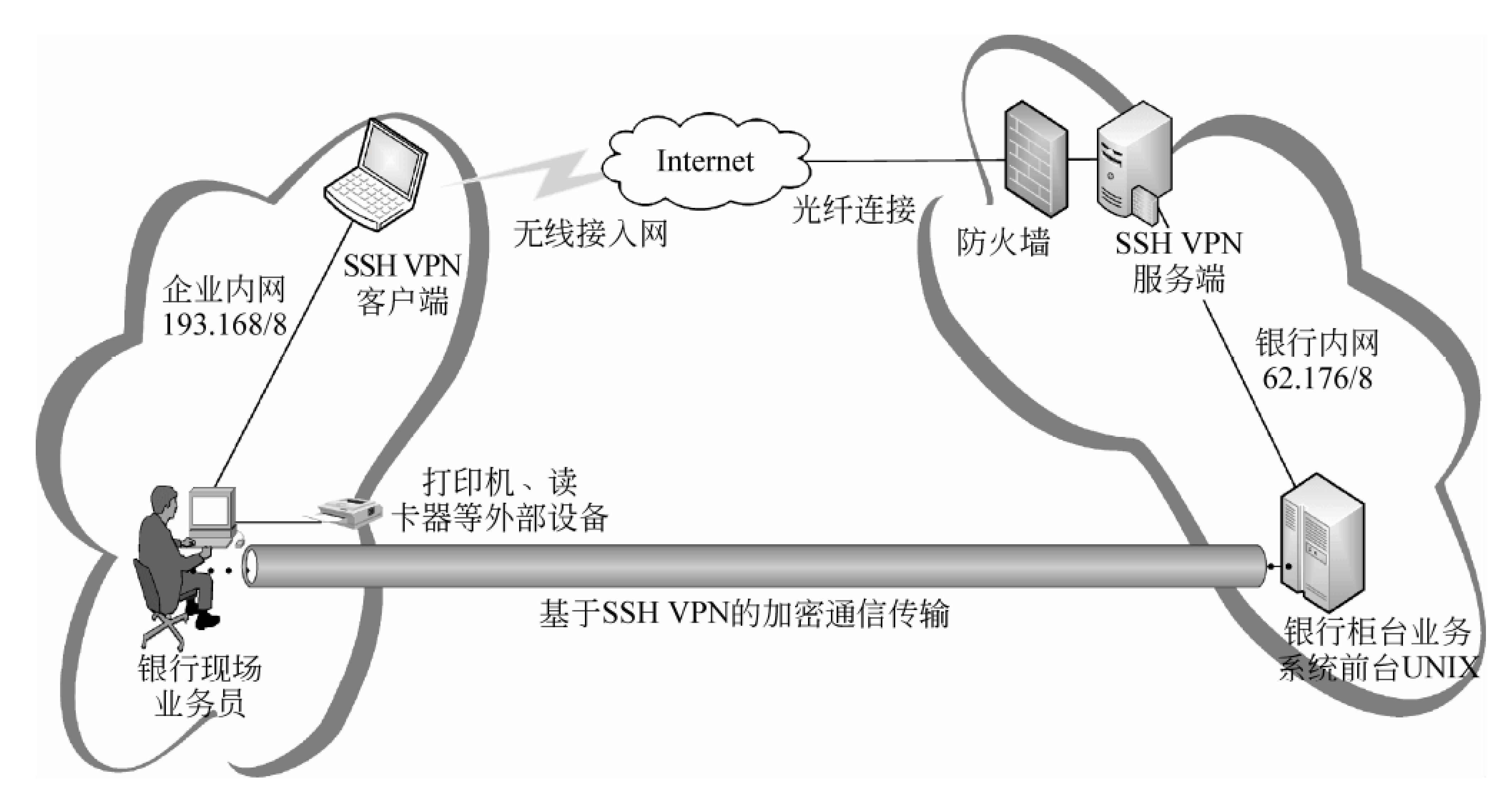


图 5-6 基于 SSH 协议实现的银行无线移动柜台

软件，该服务器装有两块网卡，一块经过防火墙连接因特网，另一块通过内部专网连接柜面业务系统前台 UNIX 主机。OpenSSH 服务进程从因特网接收无线移动柜台上传来，经过 SSH 协议加密的 Telnet 登录请求，经解密，将登录请求转发到柜面业务系统前台 UNIX 主机。这样，无线移动柜台就成功登录到柜面业务系统前台 UNIX 主机，成为 UNIX 主机的一个远程终端，可以运行柜面业务系统前台程序，办理银行业务。这就相当于利用 SSH，在银行现场业务员和银行柜台业务系统之间建立了一条虚拟的安全通信链路。

习题 5

1. 观察并试举例说明日常工作和生活中可能使用 SSH 安全协议的例子。

2. 调研目前在计算机网络标准化领域具有重要影响力的国际标准化组织，说明目前 SSH 安全协议标准化进程由谁主导，并思考可能的原因。

3. SSH 协议是分层协议，请简述其各个层次及其功能。

4. 简述 SSH 协议面临的安全风险。

5. SSH 协议为什么要单独设计 SSH 连接协议，而不是直接在传输协议中进行连接参数协商？

第 6 章　应用层安全协议

6.1　背景介绍

Internet 是当今广泛使用的计算机网络，TCP/IP 协议则是 Internet 采用的核心网络通信协议。由于 TCP/IP 协议本身缺乏可靠的安全机制，以及 Internet 具有开放性和共享性特点，因此网络安全性就显得更加脆弱。目前，有多种网络安全的解决方案，分别实现在 TCP/IP 协议栈的不同层次上，如图 6-1 所示。在物理层上使用机械或电器方法，防止信息被非法窃取，如电磁泄漏保护；在数据链路层上使用硬件加密设备，直接加/解密链路两端的数据，或采用用于组建远程访问 VPN 的安全协议 PPTP 和 L2TP 创建安全通道；在网络层上通过基于 IPSec 规范的安全协议，实现各种方式的 VPN；在传输层使用 SSL、TLS 等安全协议，提供端对端的安全通信；在应用层则可以实现对某些特殊服务进行单独保护，如 S-MIME、PEM、PGP、S-HTTP、SET 等。本书主要关注于网络安全协议，所以对物理层上的安全措施没有涉及。在前面章节中，我们分别对应用层以下的安全措施作了相应介绍，本章将着重介绍应用层的安全协议。

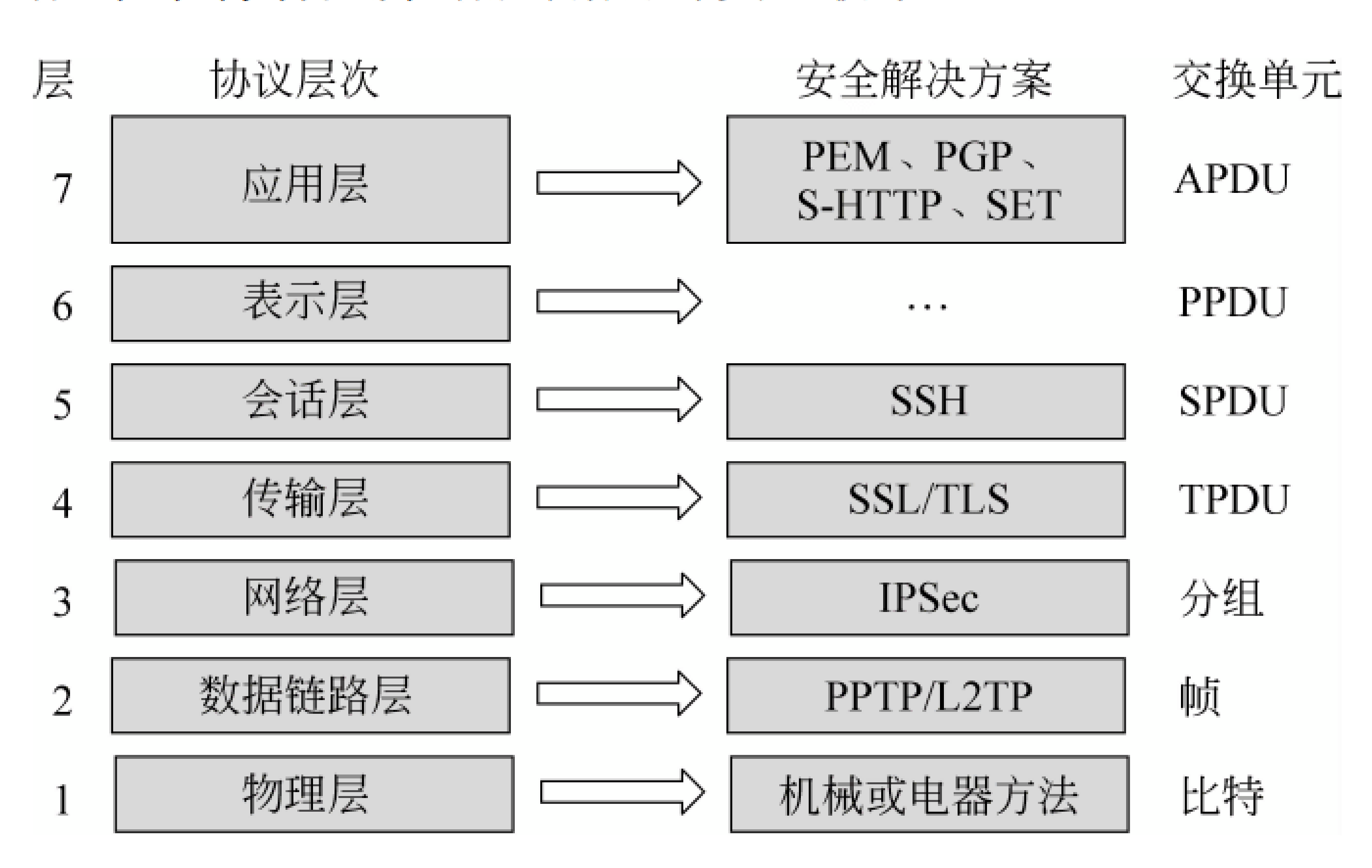


图 6-1　不同网络层次安全解决方案示意图

6.2　应用层安全威胁

据《第 29 次中国互联网络发展状况统计报告(2012 年 1 月版)》公布的数据显示，截至 2011 年 12 月底，中国网络用户规模突破 5 亿，互联网普及率较 2010 年提升 4 个百分点。截至 2011 年底，中国网站规模达到 229.6 万，较 2010 年底增长 20%，有望进入一个新的增长周期。与此同时，国家顶级域名.CN 的注册量也开始转身向上：2011 年底.CN 域名注册量达到 353 万个，较 2011 年中增长 26000 余个。网站规模的回升，一方面得益于传统企业对互联网的重视、建设和应用推进；另一方面，网站规模的回升，是泡沫被挤

压、水分被蒸发之后的回升,中国的互联网产业将更加健康,网络应用将更加扎实,发展也将更加稳健。随着网络的真正普及,电子商务类应用使用率保持上升态势。电子商务类应用稳步发展,网络购物、网上支付、网上银行和在线旅行预订等应用的用户规模全面增长。与2010年相比,网购用户增长3344万人,增长率达到20.8%,网上支付、网上银行使用率也增长至32.5%和32.4%。另外,团购成为全年增长第二快的网络服务,用户年增速高达244.8%,用户规模达到6465万,使用率提升至12.6%。截至2011年12月底,我国使用网上支付的用户规模达到1.67亿,使用率提升至32.5%。与2010年相比,用户增长2957万,增长率为21.6%。中国互联网应用的消费商务化特征走强趋势明显。但与此同时,网络应用的安全形势却不容乐观。因此下面介绍一些在应用层基础上增加安全协商算法和数据加密的安全协议,包括S-MIME、S-HTTP协议等。

6.3 电子邮件安全协议

6.3.1 MIME协议

多用途互联网邮件扩展(Multipurpose Internet Mail Extensions,MIME)是当前广泛应用的一种电子邮件技术规范,基本内容定义于RFC 2045~RFC 2049(注意:RFC 1521和RFC 1522是它的历史版本)。

MIME试图在不改变SMTP协议和RFC822(邮件格式标准)的基础上,使邮件可以传送任意二进制文件。图6-2给出了一个典型的MIME协议连接响应示意图。

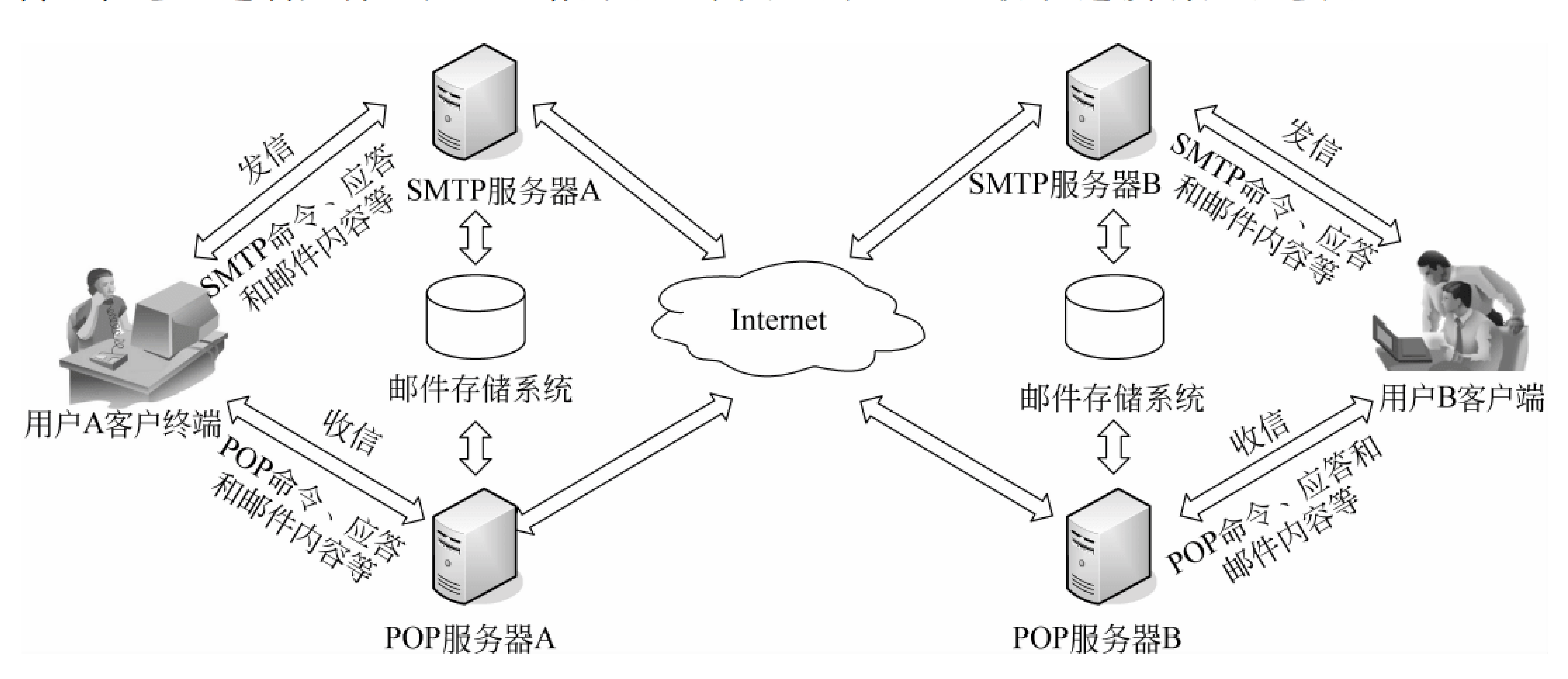


图6-2 MIME协议连接响应示意图

6.3.2 电子邮件安全威胁

电子邮件的出现使人们再一次认识到享受一件事情所带来的方便和快捷的同时,也不得不面对其可能被滥用而导致的风险。作为目前互联网上应用最多的服务,电子邮件

在 Internet 上的传输却是没有任何保密措施的。电子邮件以不加密的“明文”形式，从一个网络传到另一个网络，最终达到目的网络。这使得用户的电子邮件有可能被人偷窥、篡改和仿冒，造成重要信息的泄露。电子邮件的安全保密问题已越来越引起人们的担忧，目前常见威胁包括垃圾邮件、密码泄露、网络嗅探等。

垃圾邮件威胁是一个古老的话题。正如人们无法确定是谁发出世界上第一封电子邮件一样，第一封垃圾邮件发出的确切时间、地点及人物均有争议。但毫无疑问的是，垃圾邮件的出现使得文献可查最早用 spam 来指代垃圾邮件这种“不请自来、匿名的、商业群发信息”的是 Joel Furr，用来描述 1993 年 ARMM 系统缺陷所导致的邮件滥发事件，这一指代也在 IETF RFC 2635 标准中得以承认。从那时起，研究者就投入到对抗垃圾邮件的战斗中，几乎模式识别领域的所有技术，包括 SVM、决策树、Bayes 理论、模糊理论、智能计算、神经网络、推理技术等，都被用来阻止垃圾邮件的传播泛滥。近年来，随着因特网的迅猛发展，垃圾邮件泛滥问题已经成为虚拟世界的巨大难题和挑战，迅速增长的垃圾邮件已经给网络用户和运营商造成了巨大损失（网络带宽和用户精力的双重损失）。我们迫切需要从法律层面和技术层面采取措施，防治垃圾邮件肆虐。目前，一些商用的垃圾邮件过滤器已经进入市场，如 D2S（Death2Spam）、SpamBayes、SpamProbe、Bogofilter、DSPAM、CRM114 Discriminator 以及 Spamassassin。

密码泄露会严重威胁到电子邮件服务的安全。很多用户都知道密码的重要性，也知道越复杂密码的安全性就越高。但在实际应用中，人们往往选择更容易记忆的密码而非更安全的密码。据英国《每日电讯报》报道，互联网数据应用安全公司 Imperva 通过研究数千万网友的网络账号信息，总结出 10 大最常用网络密码。这 10 大最烂密码分别为 123456、12345、123456789、Password、iloveyou、princess、rockyou、1234567、12345678 和 abc123。破解者最容易想到的就是生日、用户名、电话号码、QQ 号码等，显然，这些是人们生活中最容易记住的，但也是最容易被破解掉的。其实，在字母中夹杂数字、符号和区分大小写形式，可以在一定程度上提升密码的安全性。

网络嗅探简单易行但威胁巨大。电子邮件以不加密的“明文”形式，从一个网络传到另一个网络，最终达到目的网络。通过网络嗅探，就能够获取用户数据，进而威胁用户安全。通常，攻击者使用嗅探器，对局域网内传输的数据进行监听，因为 POP3 协议都是明文传输，所以通过嗅探捕获的数据，很容易分析出用户密码和传输内容。

电子邮件协议设计的初衷主要考虑了邮件服务的开放性和共享性，忽略了安全机制的保障。电子邮件协议的安全性存在先天不足，使邮件内容随时都可能被某些别有用心的人偷窥、复制、篡改或者仿冒。因此，对现有的电子邮件协议进行安全增强，是十分必要的。特别是当用户电子邮件涉及重要信息、敏感信息和个人隐私时，就更需要采取相应手段来保证邮件安全了。安全电子邮件能解决邮件的加密传输问题，验证发送者的身份验证问题，错发用户的收件无效问题（因为需要用密钥解密），下面将介绍 S/MIME（Secure Multi-Part Intermail Mail Extension）和 PGP（Pretty Good Privacy）这两种保证电子邮件安全常用到的安全技术。S-MIME 和 PGP 这两种协议对一般用户来说是透明的，在使用上几乎没有什么差别，但它们的协议格式不同，无法互联互通。

6.3.3 S/MIME 协议

S/MIME 协议的最初版本来源于 RSA 数据安全公司。S/MIME v2 版本已经广泛应用在安全电子邮件上，得到产界业广泛认可，微软公司、Novell 公司等都支持该协议。但是 S/MIME 协议并不是 IETF 的标准，需要使用 RSA 算法进行的密钥交换，限于美国 RSA 数据安全公司的专利。

S/MIME 是从 PEM（Privacy Enhanced Mail，邮件私密性增强协议）和 MIME（Multipurpose Internet Mail Extensions，多用途网际邮件扩充协议）发展而来的。MIME 说明了如何安排消息格式，使消息在不同的邮件系统内进行交换。MIME 的格式灵活，允许邮件中包含任意类型的文件。MIME 消息可以包含文本、图像、声音、视频及其他应用程序的特定数据。具体来说，MIME 允许邮件的单个消息中可含多个对象、文本文档不限制一行长度或全文长度、可传输 ASCII 以外的字符集，允许非英语语种的消息、多字体消息、二进制或特定应用程序文件、图像、声音、视频及多媒体消息。MIME 是正式的 Internet 电子邮件扩充标准格式，但它未提供任何安全服务功能。PEM 协议（可见 RFC 1421、RFC 1422、RFC 1423 和 RFC 1424）在 Internet 电子邮件的标准格式上增加了加密、鉴别和密钥管理的功能，允许使用公开密钥和专用密钥的加密方式，并能够支持多种加密工具。对于每个电子邮件报文，可以在报文头中规定特定的加密算法、数字鉴别算法、散列功能等安全措施。S/MIME 协议正是借鉴 PEM 邮件私密性增强协议，在 MIME 上定义安全服务措施的实施方式，从而增强电子邮件的安全性。

在国外，VeriSign 向个人提供 S/MIME 电子邮件证书；在国内，则有北京天威诚信（iTrus China）公司提供支持该标准的产品。而在客户端，Netscape Messenger 和 Microsoft Outlook 都支持 S/MIME。图 6-3～图 6-8 以北京天威诚信公司安全电子邮件证书申请为例，展示了申请和使用个人安全电子邮件证书的过程。



图 6-3 访问安全电子邮件证书中心



图 6-4　注册个人安全电子邮件证书



图 6-5　确认电子邮件地址

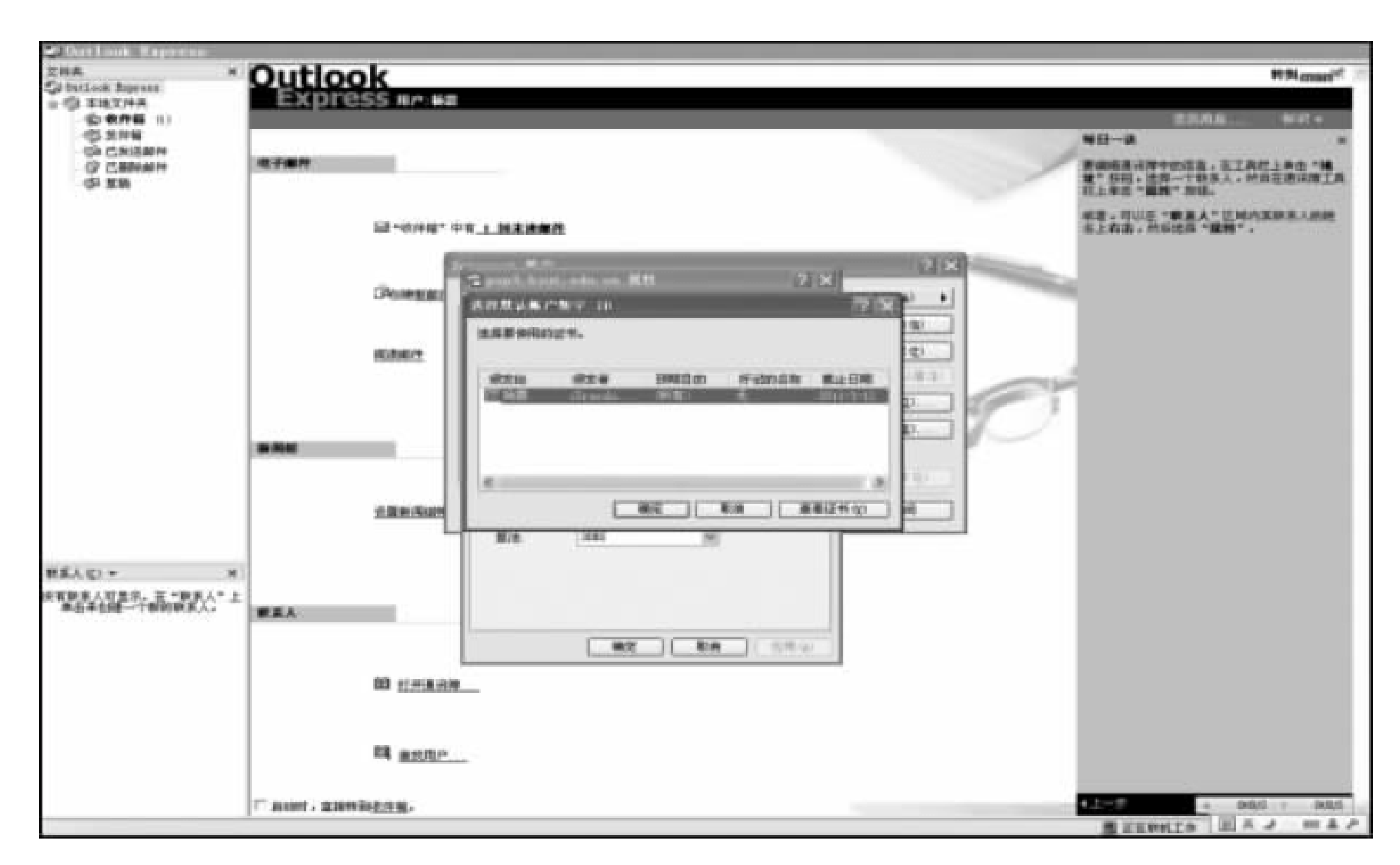


图 6-6　管理员批准证书



图 6-7 发送加密的电子邮件

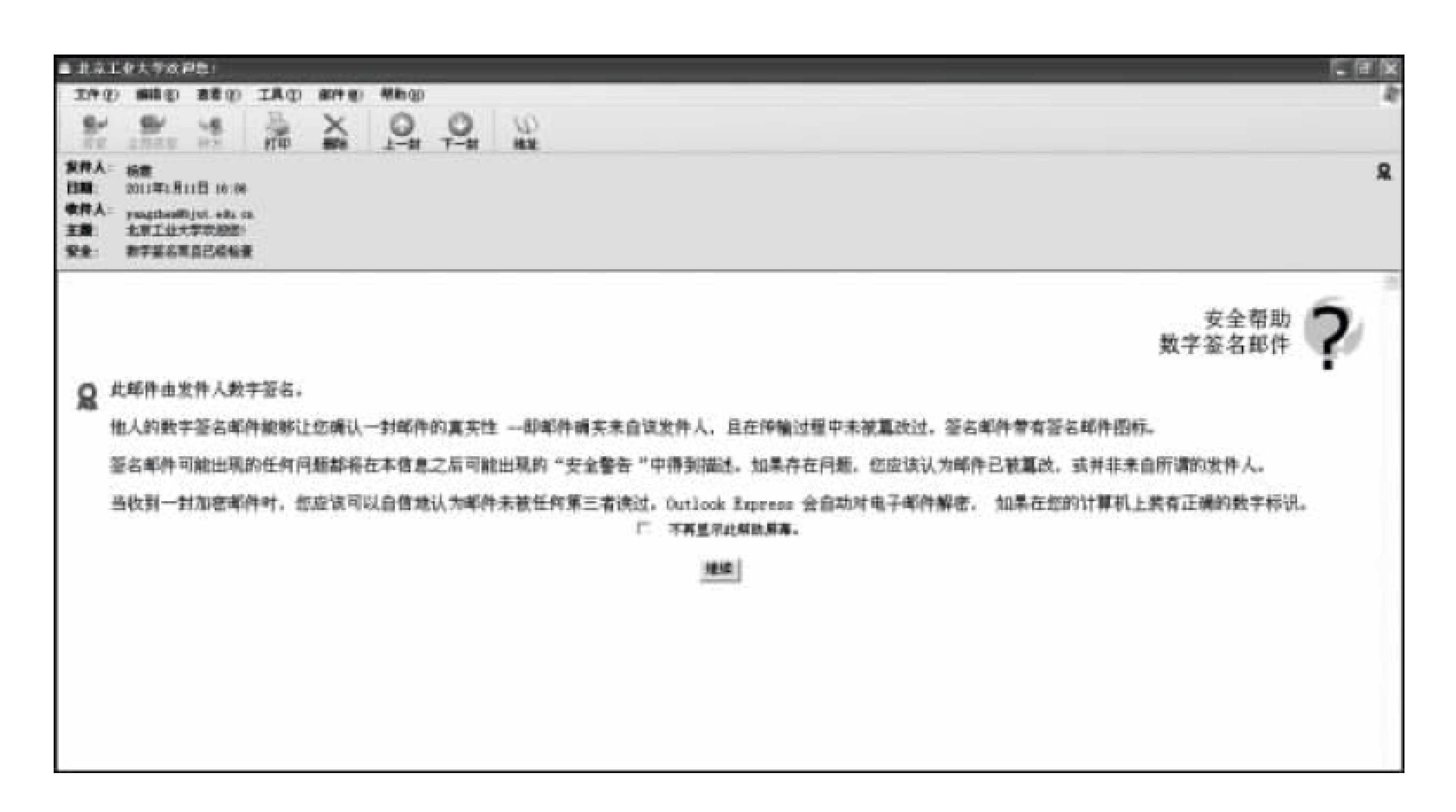


图 6-8 发送带数字签名的邮件

6.3.4 PGP 协议

1. PGP 协议简介

PGP 加密虽然并不是 Internet 标准，但同 S/MIME 一样，也是目前应用广泛的电子邮件加密方式。PGP 最早出现在 1990 年，是一种长期在学术圈和技术圈内得到广泛使用的安全邮件标准。其特点是通过单向散列算法对邮件内容进行签名，保证信件内容无法修改。PGP 是一种对电子邮件进行加密和签名保护的安全协议和软件工具，它创造性地将基于公钥密码体制的 RSA 算法和基于单密钥体制的 IDEA 算法巧妙地结合起来，同时兼顾了公钥密码体系的便利性和传统密码体系的高速度，形成一种高效的混合密码系统。

发送方使用随机生成的会话密钥和 IDEA 算法加密邮件文件，使用 RSA 算法和接收方的公钥加密会话密钥，然后将加密的邮件文件和会话密钥发送给接收方。接收方使用自己的私钥和 RSA 算法解密会话密钥，然后再用会话密钥和 IDEA 算法解密邮件文件。

它的特点如下。

(1) PGP采用了基于数字签名的身份认证技术。对于每个邮件,PGP使用MD5算法产生一个128位的散列值,作为该邮件的唯一标识,并以此作为邮件签名和签名验证的基础。

然后把它附加在邮件后面,再用B的公钥加密整个邮件。

B收到加密的邮件后,首先使用自己的私钥解密邮件,得到A的邮件原文和签名,然后使用MD5算法产生一个128位的散列值,并和解密后的签名相比较。如果两者相符合,则说明该邮件确实是A寄来的。

(2) PGP还允许对邮件只签名不加密。这种情况适用于发信人公开发表声明的场合。发信人为了证实自己的身份,可以用自己的私钥签名。收件人用发信人的公钥来验证签名,不仅可以确认发信人的身份,还可以防止发信人抵赖自己的声明。

(3) PGP采用IDEA算法加密邮件内容。IDEA算法是单密钥算法,加密和解密共享一个密钥。发信人首先随机生成一个密钥,使用IDEA算法加密邮件内容,然后再利用RSA算法加密该随机密钥,并随邮件一起发送给收件人。收件人首先用RSA算法解密出该随机密钥,再用IDEA算法解密出邮件内容。

例如,为了证实邮件是A发给B的,A首先使用MD5算法产生一个128位的散列值,再用A的私钥加密该值,作为该邮件的数字签名。

在PGP中,采用公钥密码体制来解决密钥分发和管理问题。公钥是公开的,不存在监听问题,但公钥的发布仍有一定的安全风险。举例如下。

假如A要给B发邮件,必须首先获得B的公钥,A从第三方上下载B的公钥,然后用它加密邮件,并用E-mail系统发给B。然而在A和B都不知道的情况下,另一个C假冒B的名字,生成一个密钥对,并在第三方中用自己生成的公钥替换了B的公钥。结果A从第三方上得到的公钥便是C的,而不是B的。

于是便出现了下列风险。

(1) C可以用它的私钥来解密A给B的邮件。

(2) C可以用B的公钥来转发A给B的邮件,并且谁都不会起疑心。

(3) C可以改动邮件的内容。

(4) C可以伪造B的签名,给A或其他人发邮件,因为这些人拥有的公钥是C伪造的,他们会以为是B的来信。

为了防止这种情况发生,可以采用如下方法。

(1) 直接从对方手中得到他的公钥。

(2) 通过认证中心得到公钥。

(3) 密钥可以通过电话认证。

(4) 密钥指纹标识。

2. PGP的下载与安装

目前,PGP的最新版本是9.0,支持的系统包括Amiga、Atari、BeOS、EPOC (Psion etc.)、Mac OS、MS-DOS、Newton、OS/2、PalmOS、UNIX、Windows 2000、Windows 3.x、

Windows 95/98/NT/ME/XP。用户可以从以下地址获得该软件：http://www.pgp.com/、http://www.pgpi.com/、http://www.mantis.co.uk/pgp/pgp.html。

PGP 的安装过程如下。如图 6-9～图 6-12 所示。

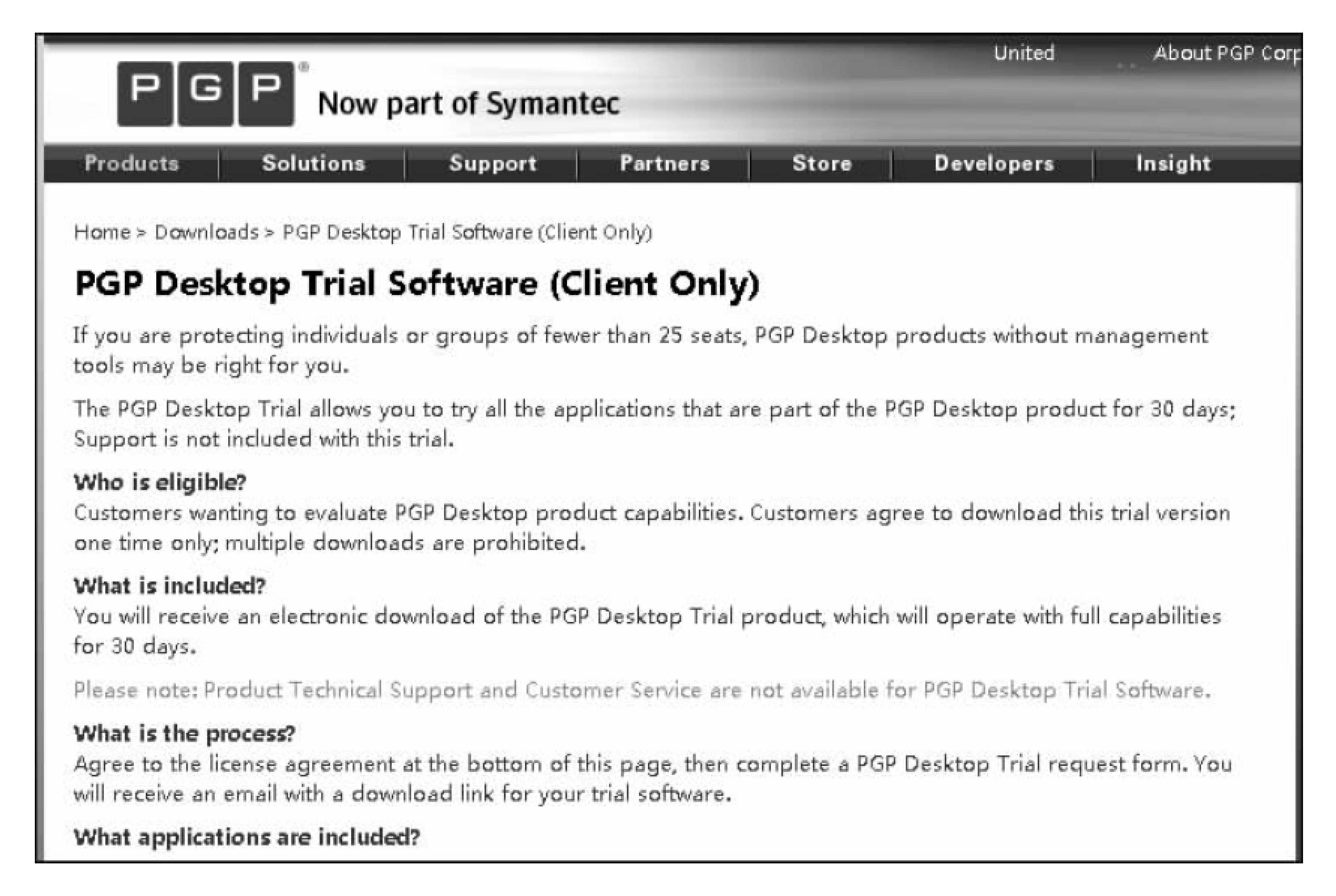


图 6-9　访问 PGP 网站下载软件



图 6-10　选择安装 PGP 组件

(1) 跳过欢迎界面，在下一对话框中的 Full Name 项目中输入名字，不必输入真实姓名，可以输入常用的网名等；然后在 Email Address 项目中输入自己的邮件地址，这一地址应是别人给用户写信时所填写的地址，即公开的邮件地址，完成后单击“下一步”按钮。

(2) 接下来的对话框要求用户输入保护私钥的 PIN 码，因为私钥在默认情况下是保存在硬盘上的，所以需要一个 PIN 码对它进行保护，这样需要使用私钥时(例如签名或打

开加密邮件)，系统就会首先要求用户输入 PIN 码。实际上，为了使私钥更加安全，用户可以不把它保存到硬盘上，而将其放置在 USB 介质上，这样就可以像使用信用卡一样方便和随心了。同时，为了更好地保护私钥，密码至少要输入 8 个字符，并且应该包含非字母字符。完成后，单击“下一步”按钮。

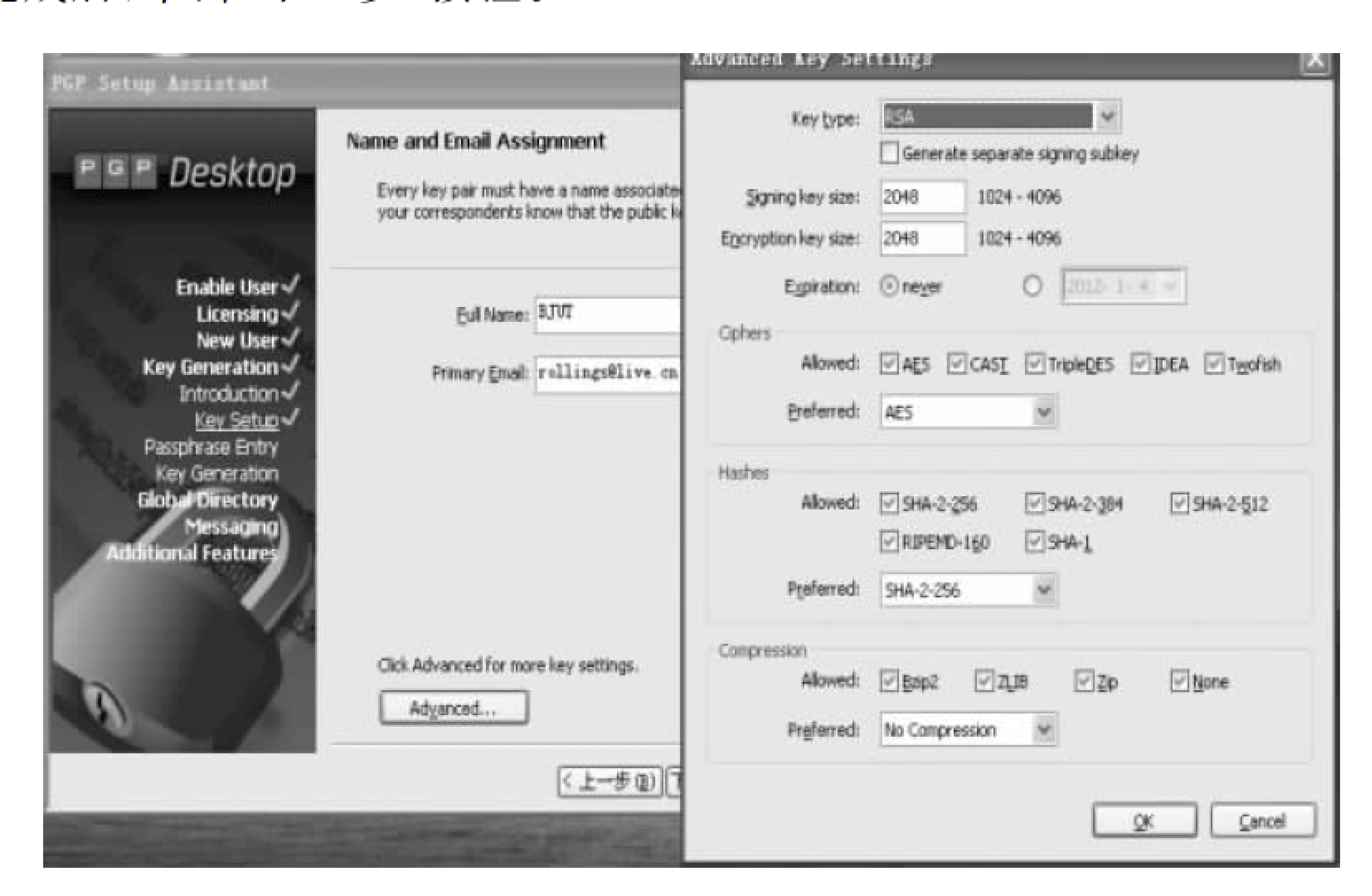


图 6-11　生成密钥对

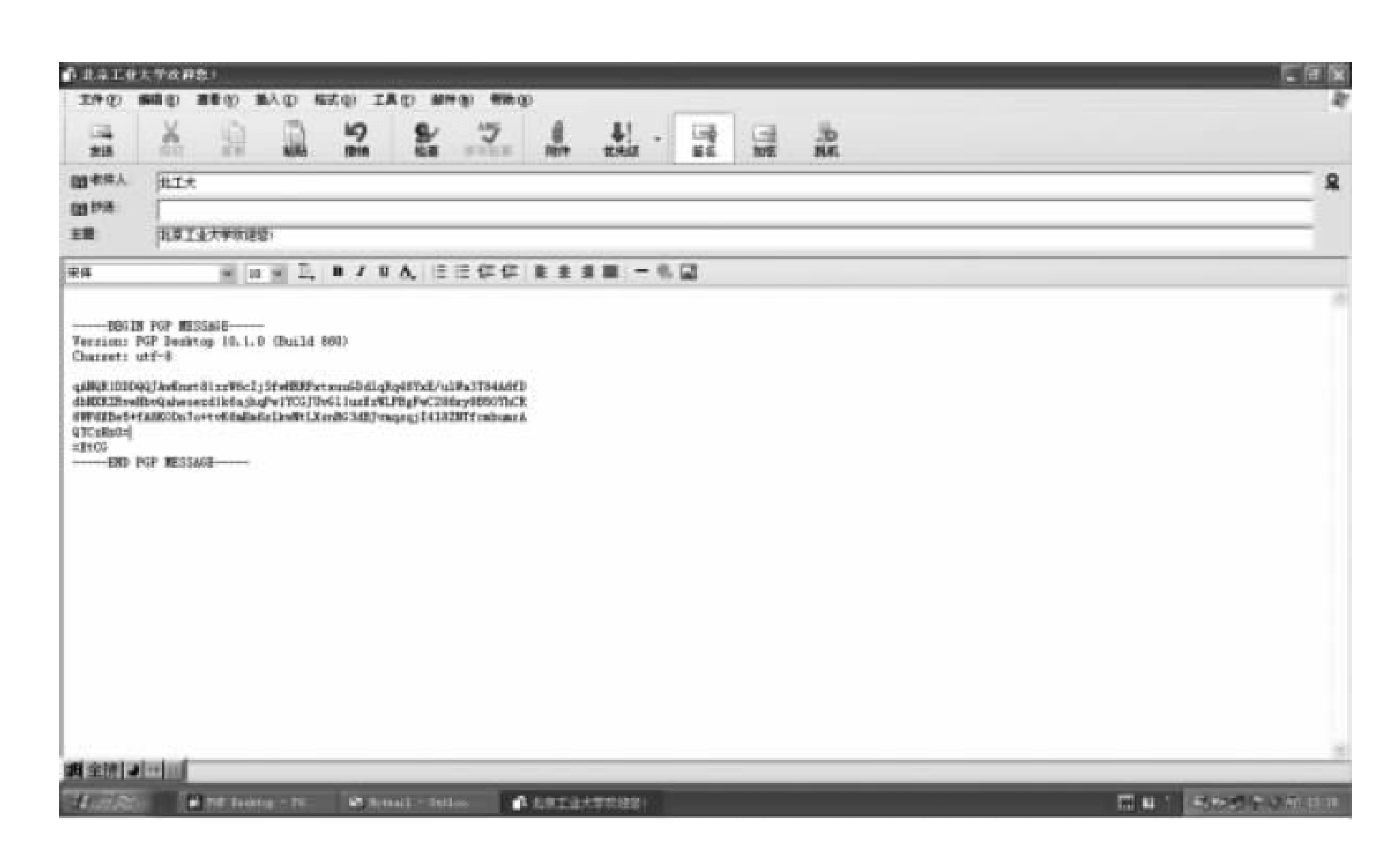


图 6-12　使用 PGP 加密个人邮件

用户可以通过电子邮件，把自己的公钥分发给朋友，但推荐用户还是把自己的公钥发送到公钥服务器上，发送邮件时直接通过 Internet 查找并下载，这样即使系统崩溃也不会丢失公钥。要把公钥发送到公钥服务器上，选择“开始”|“程序”|PGPkeys，选中相关密钥后，继续选择 Server|Send to|Domain Server 即可。这一公钥服务器是由 PGP 公司提供的，地址为 keyserver. pgp. com。

以在 Outlook Express 中加密邮件为例。由于安装了 Outlook Express 的 PGP 插件，所以加密邮件的过程非常简单，只要在发送邮件前单击 Encrypt Message (PGP)按钮

即可。如果要对邮件进行签名，可以同时单击 Sign Message(PGP)按钮。在单击“发送”按钮后，PGP 会根据收件人的地址自动连接公钥服务器，去获取这一地址所对应的公钥，然后用它加密邮件并发送。如果发送邮件前单击 Sign Message (PGP)按钮，系统还会提示用户输入保护私钥的 PIN 码。例如，输入表 6-1 中的左栏内容，则加密后邮件将显示为右栏所示内容。

表 6-1　邮件加密前后内容显示的变化

原始邮件	加密后邮件
您好！ 北京工业大学欢迎您！ 致 礼！ 北京工业大学 2011 年 1 月 1 日	qANQR1DDDQQJAwKnxt81zzW6cZjSfwHRRFxtxuuGDdlqRq 48YxE/ulWa3T84A6fD dbNXRZRveHbvQaheoezd1k6ajhqPw1YCGJUvGl1usXzWLPBgFwC 286xy9B5OYhCR 6WF6XBe5 ＋ fA8KODn7o ＋ tvK6mEm6slkwNtLXsnRG3d- BJvmqsqjI4l8ZNTfcmbumrA QTCzHz0＝ ＝XtCG

PGP 可以用以下方式管理密钥。

(1) 将私钥保存到闪盘中。选择 Edit|Options，在弹出的对话框中进入“Files”选项卡，查看私钥当前的保存路径。然后将私钥移动到闪盘中，最后在此对话框中把私钥的保存路径改为闪盘的文件路径即可。

(2) 导出公钥，以发送给朋友。选择 Keys|Export，且在弹出的对话框中不选中 include private keys 选项即可。PGP 公司提供了公开钥匙服务器的统一地址，内容如下。

电子邮件：pgp-public-keys@keys. pgp. net。

Web 地址：http://www. pgp. net/pgp/www-key. html。

匿名文件传输协议：http://ftp. pgp. net/pub/pgp。

3. PGP 的安全性

(1) 加密体系安全性。指加密体系中各个加密算法本身的坚固性和抗攻击能力。PGP 的加密体系由 4 个关键部分组成：对称加密算法(IDEA)、非对称加密算法(RSA)、单向散列算法(MD5)和随机数产生器。

(2) 实现系统的安全性。指一个 PGP 实现系统是否存在可能被攻击者利用的系统安全漏洞以及如何堵塞漏洞。

① IDEA 算法的安全性。IDEA 算法是用来加密邮件内容的，对于采用直接攻击法的破译者来说，IDEA 是 PGP 密文邮件的第一道防线。

对一个密码算法的攻击主要有两种方法，密码分析方法和密钥穷举法。密码分析的方法是通过分析密码算法的弱点来破译密文；密码穷举法是通过穷举搜索找出密钥来破译密文。

由于 IDEA 的密钥空间是 128 位，穷举的时间很长，更何况 PGP 采用随机产生密钥的方法，即使一个 IDEA 密钥失密，也只能泄露一次加密信息，并不会影响下一次加密的

信息，也不影响 RSA 密钥对的保密性。

IDEA 的安全性还与密钥随机生成器的随机特性有关。如果随机密钥生成算法生成的密钥过于“规律”，没有均匀分布到整个密钥空间上，则可能产生漏洞。

② RSA 算法的安全性。RSA 使用了两个非常大的素数的乘积，就目前的计算机水平和能力是无法分解的。但这并不能证明 RSA 的安全性，因为大数分解不一定是攻击 RSA 的唯一途径。RSA 可能存在一些密码学方面的缺陷，随着大数分解技术的发展、计算机能力的提高和计算机造价的降低，可能会威胁 RSA 的安全性。但目前来看，RSA 还是比较安全的。

③ MD5 算法的安全性。在 PGP 中，MD5 算法主要用于对用户口令和邮件签名的散列保护。一个单向散列算法的强度主要表现为对任意输入数据所散列的随机化程度，并且能产生唯一输出。如果要破译 MD5 所散列的 128 结果，必须有足够的计算能力，并且将耗费巨大的代价。

④ 随机数的安全性。在 PGP 中，每次加密数据的密钥是一个随机数，而计算机是无法产生真正随机数的，只能产生近似随机数的伪随机数。PGP 对随机数的产生是很谨慎的，对于关键随机数的产生，是从用户敲击键盘的时间间隔上获取随机数种子的。对于键盘上的 randseed. bin 文件，也采用了与邮件同样强度的密码进行加密，这就有效防止了攻击者从 randseed. bin 文件中分析出加密密钥的产生规律。

PGP 用户指南中说它是一种混合密码系统：当用户利用 PGP 加密明文，数据首先被压缩，节省了传送时间和硬盘空间，更重要的是增强了加密安全。大多数加密技术用镶嵌在明文中的模板来解密，压缩减少了明文中的模板，大大增强了密码破解的难度。

然后，PGP 生成一个 Session Key，这个密钥是一次性的，由鼠标移动和按键随机产生。数据一旦被加密，Session Key 就被加密到接收者的公钥中，并与暗记文一起传送给接收者。解密的过程相反。利用私钥获得接收到的 PGP 副本中的临时 Session Key，然后 PGP 利用它解密加密的暗记文。

6.4 S-HTTP 协议

6.4.1 HTTP 协议

Web 浏览器与服务器之间遵循 HTTP 协议进行通信传输。HTTP（Hyper Text Transfer Protocol，超文本传输协议）是分布式的 Web 应用的核心技术协议，在 TCP/IP 协议栈中属于应用层。它定义了 Web 浏览器向 Web 服务器发送索取 Web 页面请求的格式，以及 Web 页面在 Internet 上的传输方式。另外，HTTP 还能维持多媒体信息的完整性，可以说是 Web 上图像、音频、视频、超文本等信息的传输载体。Web 之所以把 HTTP 当做其基本协议，是因为没有其他协议能提供如此全面的性能。

HTTP 是一个基于消息的协议。它有两部分消息，一部分是从浏览器（客户端）发往服务器的请求，另一部分是服务器对客户端的响应。HTTP 分 4 步完成一次事务，如图 6-13 所示。

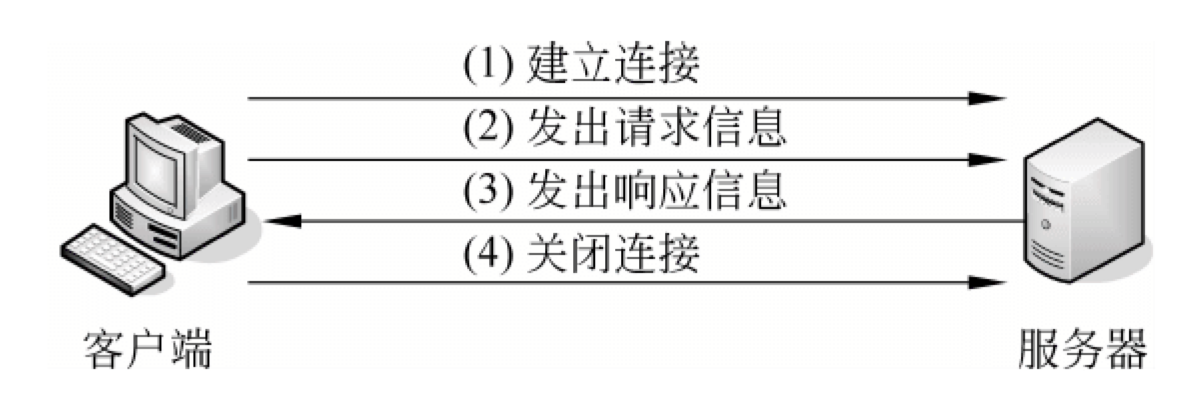


图 6-13　HTTP 协议连接响应示意图

(1) Web 浏览器和服务器之间建立 TCP/IP 连接。Web 浏览器和服务器之间的连接是通过套接字实现的。客户打开一个套接字,并把它绑定在一个端口上,如果成功,就相当于建立了一个虚拟文件,以后就可以在该虚拟文件上写数据,并通过网络向外传送。

(2) 浏览器(客户端)向服务器发出请求。建立连接后,客户机把请求消息发送到服务器的监听端口上,完成提出请求操作。请求消息格式如图 6-14 所示。

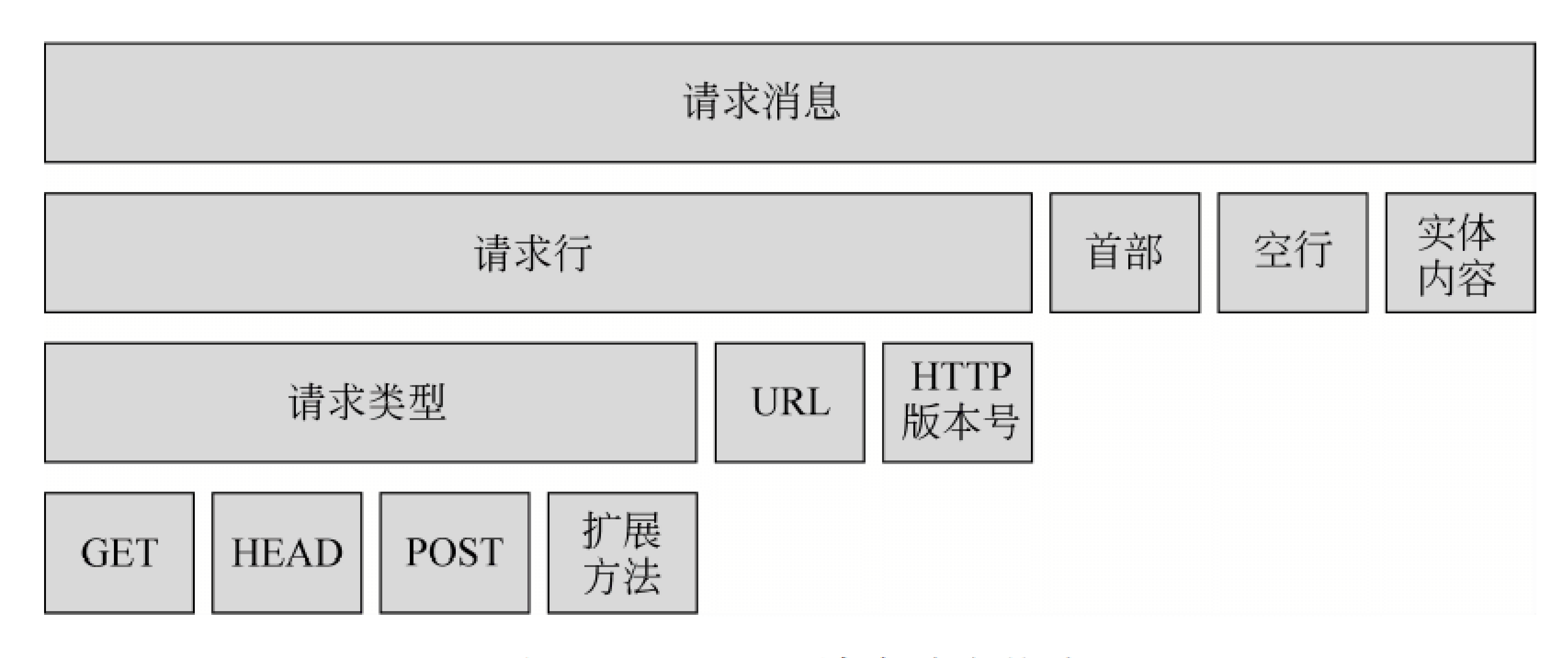


图 6-14　HTTP 请求消息格式

请求消息=请求行+首部+空行+[实体内容]

请求行包含:请求类型、URL、HTTP 版本号

(1) 请求类型=GET|HEAD|POST|扩展方法。

① GET。不同的请求对象对应 GET 的结果不同,对应关系如表 6-2 所示。

表 6-2　不同的请求对象对应 GET 的结果

对　象	GET 的结果
文件	文件的内容
程序	该程序的执行结果
数据库查询	查询结果

② POST。从客户机向服务器传送数据,在要求服务器和 CGI 做进一步处理时会用到 POST 方法。POST 主要用于发送 HTML 文本中 FORM 的内容,让 CGI 程序处理。

(2) URL。统一资源定位符。

以 http://www.bjupt.edu.cn/computer/index.htm 为例。http://代表超文本传输协议;www 代表一个 Web 服务器;bjut.edu.cn 代表装有网页的服务器的域名;computer 为该服务器的子目录,就好像文件夹;index.htm 是文件夹中的一个文件。

(3) 服务器响应客户端的请求。在处理完客户的请求后,服务器要向客户机发送响应消息。

响应消息=状态行+响应头+空行+[实体内容]

状态行：状态行包含 HTTP 版本、空格、状态码、空格和状态短语。

(4) 客户端与服务器断开连接。客户和服务器双方都可以通过关闭套接字来结束 TCP/IP 对话。

6.4.2 Web 安全威胁

Web 赖以生成的环境包括计算机硬件、操作系统、计算机网络、许多的网络服务和应用，所有这些都存在安全隐患，最终威胁到 Web 的安全。Web 的安全体系结构非常复杂，主要包括以下 7 个方面。

(1) 客户端软件(即 Web 浏览器软件)的安全。

(2) 运行浏览器的计算机设备及其操作系统的安全(主机系统安全)。

(3) 客户端的局域网(LAN)。

(4) Internet。

(5) 服务器端的局域网(LAN)。

(6) 运行服务器的计算机设备及操作系统的安全(主机系统的安全)。

(7) 服务器上的 Web 服务器软件。

在分析 Web 服务器的安全性时，一定要考虑到所有这些方面。因为它们是相互联系的，每个方面都会影响到 Web 服务器的安全性。它们中安全性最差的方面决定了给定服务器的安全级别。

Web 服务器上的漏洞可以从以下 4 个方面考虑。

(1) 在 Web 服务器上不让人访问的秘密文件、目录或重要数据。

(2) 从远程用户向服务器发送信息时，特别是信用卡之类东西时，中途遭不法分子非法拦截。

(3) Web 服务器本身存在的一些漏洞，使得一些人能侵入到主机系统，破坏一些重要的数据，甚至造成系统瘫痪。

(4) CGI 安全方面的漏洞有意或无意在主机系统中遗漏(Bug)，给非法黑客创造条件；用 CGI 脚本编写的程序涉及远程用户从浏览器中输入表格(Form)，并进行像检索(Search Index)或 Form-mail 之类在主机上直接操作的命令时，或许会给 Web 主机系统造成危险。

1. 主机系统的安全需求

网络攻击者通常通过主机的访问来获取主机的访问权限。一旦攻击者突破了这个机制，就可以完成任意操作。对某个计算机来说，通常是通过口令认证机制来登录到计算机系统上。现在大部分个人计算机没有提供认证系统，也没有身份的概念，极容易被获取系统的访问权限。因此，一个没有认证机制的 PC 是 Web 服务器最不安全的平台。所以，确保主机系统的认证机制，严密地设置及管理访问口令，是主机系统抵御威胁的有力保障。

2. Web 服务器的安全需求

随着“开放系统”的发展和 Internet 的知识普及，获取使用简单、功能强大的系统安全

攻击工具是非常容易的事情。在访问 Web 站点的用户中,不少技术高超的人有足够的经验和工具来探视他们感兴趣的东西。还有,在人才流动频繁的今天,“系统有关人员”也可能因为种种原因离开原来的岗位,系统的秘密也可能随之扩散。

不同的 Web 网站有不同的安全需求。建立 Web 网站是为了更好地提供信息和服务,在一定程度上,Web 站点是其拥有者的代言人。为了满足 Web 服务器的安全需求,维护拥有者的形象和声誉,必须对各类用户访问 Web 资源的权限作严格管理;维持 Web 服务的可用性,采取积极主动的预防、检测措施,防止他人破坏造成设备、操作系统停运或服务瘫痪;确保 Web 服务器不被用做跳板,来进一步侵入内部网络和其他网,使内部网免遭破坏,同时避免不必要的麻烦甚至法律纠纷。

6.4.3 S-HTTP 协议

安全超文本传输协议(S-HTTP)是一种结合 HTTP 而设计的消息安全通信协议,是一种面向安全信息通信的协议,它可以和 HTTP 结合起来使用。S-HTTP 能与 HTTP 信息模型共存,并易于与 HTTP 应用程序相整合。

S-HTTP 协议为 HTTP 客户机和服务器提供了多种安全机制,提供安全服务选项是为了适用于万维网上各类潜在用户。S-HTTP 为客户机和服务器提供了相同的性能(同等对待请求和应答,也同等对待客户机和服务器),同时维持 HTTP 的事务模型和实施特征。S-HTTP 客户机和服务器能与某些加密信息格式标准相结合。S-HTTP 支持多种兼容方案并且与 HTTP 相兼容。使用 S-HTTP 的客户机,能够与没有使用 S-HTTP 的服务器连接,反之亦然,但是这样的通信明显不会利用 S-HTTP 安全特征。S-HTTP 不需要客户端公用密钥认证(或公用密钥),但它支持对称密钥的操作模式。这点很重要,因为这意味着即使没有要求用户拥有公用密钥,私人交易也会发生。虽然 S-HTTP 可以利用大多现有的认证系统,但 S-HTTP 的应用并不必依赖这些系统。S-HTTP 支持端对端安全事务通信。客户机可能“首先”启动安全传输(使用包头的信息),例如,它可以用来支持已填表单的加密。使用 S-HTTP,敏感的数据信息不会以明文形式在网络上发送。S-HTTP 提供了完整且灵活的加密算法、模态及相关参数。选项谈判用来决定客户机和服务器在事务模式、加密算法(用于签名的 RSA、用于加密的 DES 等)及证书选择方面取得一致意见。

在语法上,S-HTTP 报文与 HTTP 相同,由请求或状态行组成,后面是信头和主体。显然,信头各不相同并且主体密码设置更为精密。

正如 HTTP 报文,S-HTTP 报文由从客户机到服务器的请求和从服务器到客户机的响应组成。请求报文的格式如下:

请求消息=请求行+通用信息头+请求头+实体头+信息主体

为了和 HTTP 报文区分开,S-HTTP 需要特殊处理,请求行使用特殊的“安全”途径和指定协议“S-HTTP/1.4”。因此,S-HTTP 和 HTTP 可以在相同的 TCP 端口混合处理,例如端口 80。

S-HTTP 响应采用指定协议“S-HTTP/1.4”。响应报文的格式如图 6-15 所示。

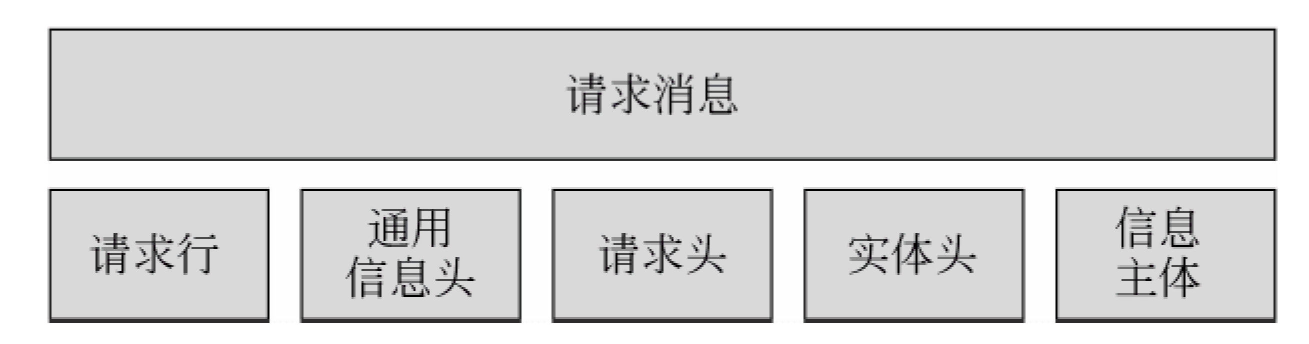


图 6-15　S-HTTP/1.4 请求消息格式

6.4.4　S-HTTP 应用实例

使用 HTTPS 协议在 Internet 上传输数据时，发送方先把数据交给 SSL 协议进行加密，再把密文由 TCP/IP 协议在网络上传输。接收方收到密文后，先提交给 SSL 协议解密成明文，再把明文进一步由 HTTP 协议处理。在这个传输过程中，数据是使用密文的形式在网络中传输的，即使黑客窃取到传输的数据，也不易破解，因此数据的安全性比较高。

要想成功架设 SSL 安全站点，关键要具备以下 4 个条件。

(1) 需要从可信的证书颁发机构 CA 获取服务器证书。

(2) 必须在 Web 服务器上安装服务器证书。

(3) 必须在 Web 服务器上启用 SSL 功能。

(4) 客户端(浏览器端)必须同 Web 服务器信任同一个证书认证机构，即需要安装 CA 证书。

具体操作步骤如下。

1. 安装证书服务

第 1 步：安装证书服务。在“开始”菜单的管理工具中选择高级管理工具，选择添加/删除 Windows 角色。在向导中找到“证书服务”，单击“下一步”按钮，添加 Active Directory 证书服务。

第 2 步：配置 CA 基本要素。分别选择 CA 类型、配置私钥、配置加密方式、配置 CA 名称、设置 CA 有效期、配置证书数据库。

第 3 步：完成 CA 服务安装。确认配置选择后，完成 CA 安装。Active Directory 证书服务用于创建证书颁发机构和相关的角色服务。基于这样的服务，用户可以颁发和管理在各种应用程序中所使用的证书。具体步骤如图 6-16～图 6-27 所示。

2. Web 服务器证书申请与配置

第 1 步：配置 IIS 服务组件。默认情况下 IIS7 组件并不安装在 Windows Server 2008 中，如果没有该组件请自行安装。

第 2 步：在 Web 服务器上为站点申请证书。

(1) 创建证书申请。单击 Web 服务器上站点名称，找到 IIS 选项下的服务器证书选项，在右边的操作中选择创建证书申请。填写证书申请，选择加密程序，将生产的证书申



图 6-16 添加 Active Directory 证书服务



图 6-17 证书服务简要说明



图 6-18 安装证书服务功能

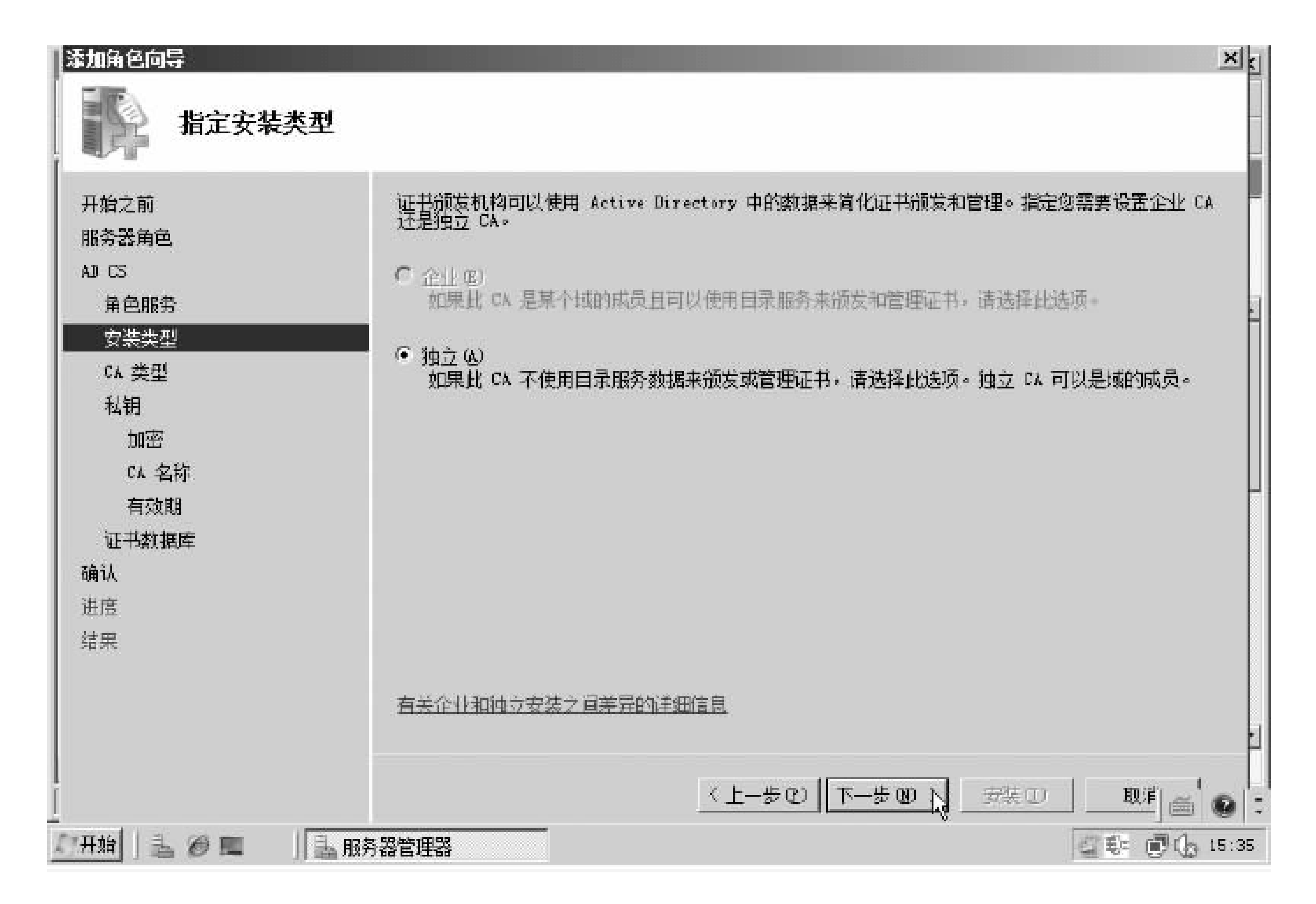


图 6-19　安装独立根 CA

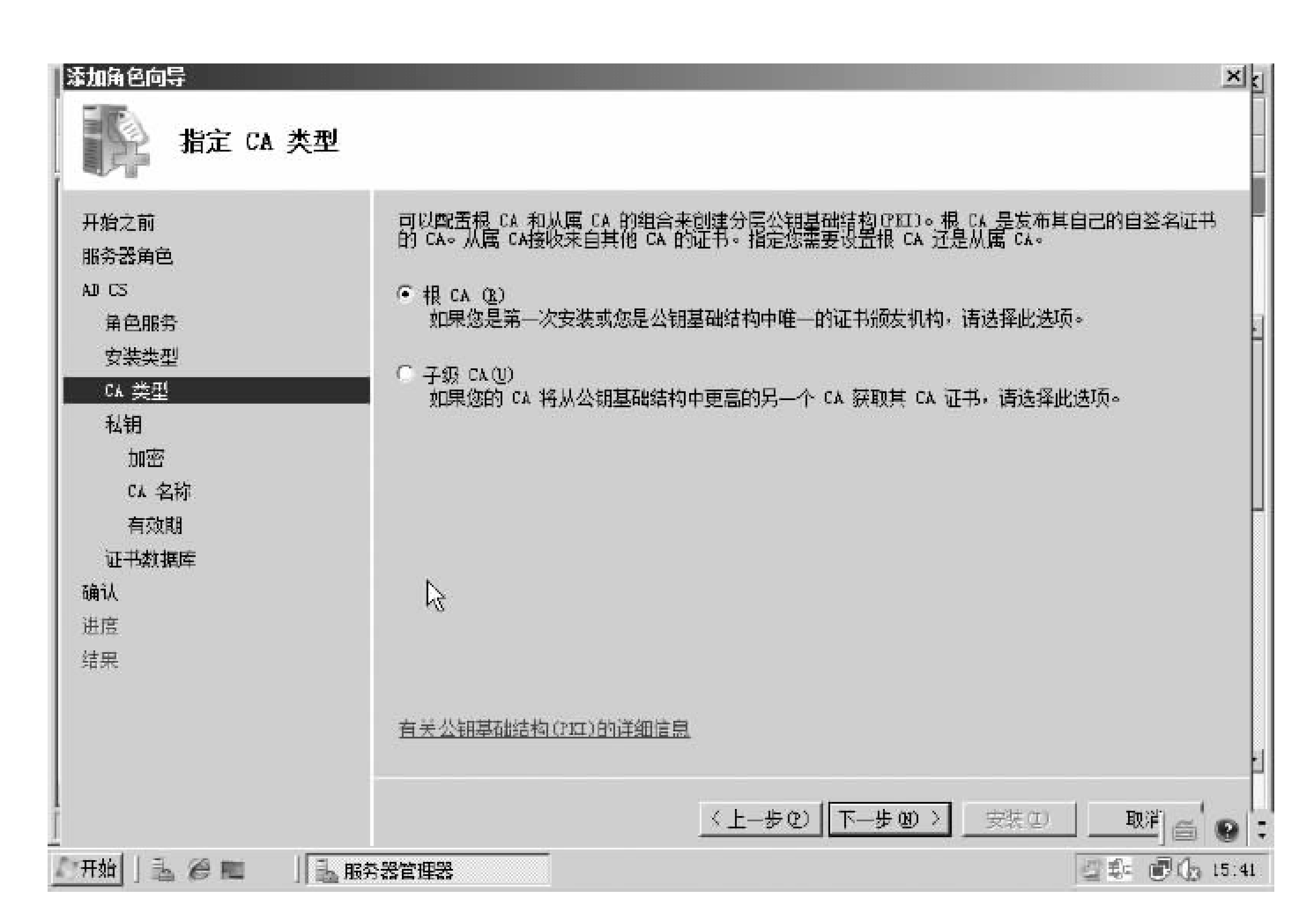


图 6-20　选择 CA 类型

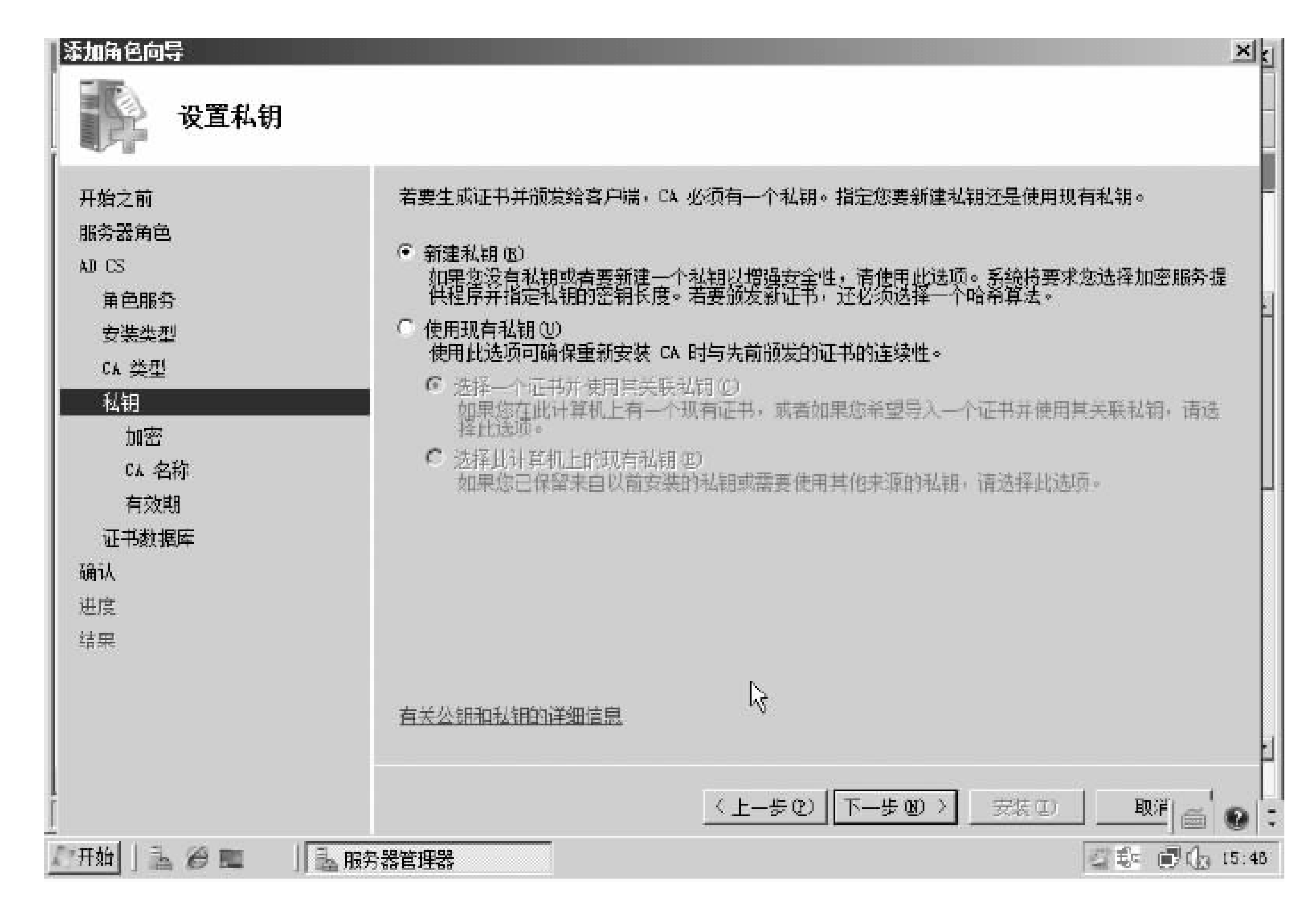


图 6-21　配置私钥

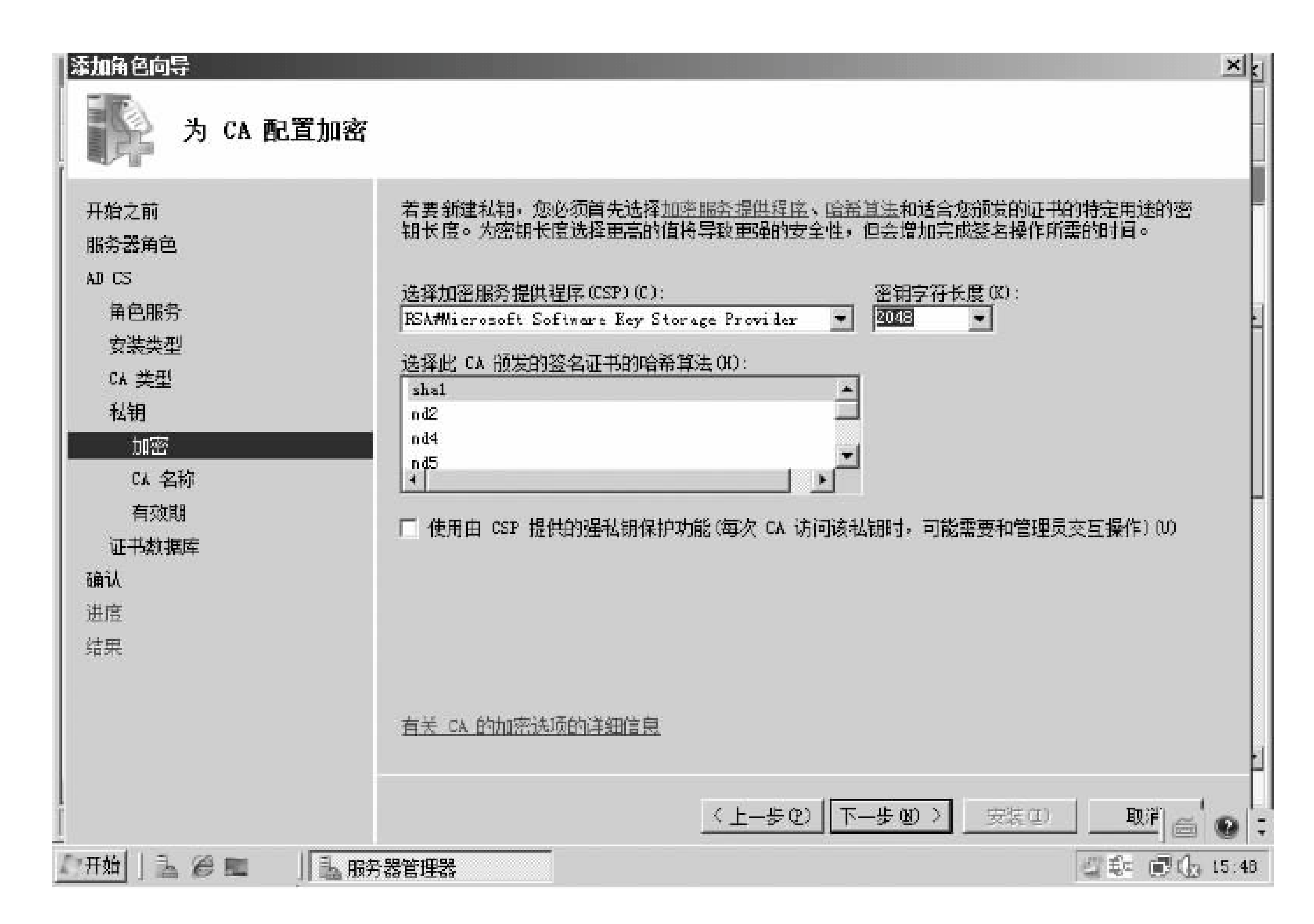


图 6-22　配置加密方式



图 6-23　配置 CA 名称



图 6-24　设置 CA 有效期



图 6-25　配置证书数据库



图 6-26　成功配置独立根 CA



图 6-27　成功安装独立根 CA

请文件保存在本地。

（2）提交证书申请。浏览器地址栏中输入 http://证书服务器地址/certsrv/，打开证书服务界面，选择高级证书申请。选择使用 base64 编码的 CMC 或 PKCS＃10 文件提交一个证书申请，提交事先存放的证书申请，等待证书服务器进一步处理。

第 3 步：在 Web 服务器上完成证书配置。

（1）等待证书颁发。成功提交申请后，证书服务器出现证书挂起提示，说明证书申请已经收到，等待管理员通过申请认证。

（2）下载颁发证书。证书服务器批准证书申请后，在 Web 服务器上下载证书。

（3）完成证书申请。单击 Web 服务器上站点名称，找到 IIS 选项下的服务器证书选项，在右边的操作中选择完成证书申请。按系统引导，导入 Web 服务器证书。

第 4 步：为 web 服务器网站设置使用 SSL。为 Web 网站添加一个 HTTPS 类型并选择证书，并强制使用 SSL 安全连接。具体步骤如图 6-28～图 6-46 所示。

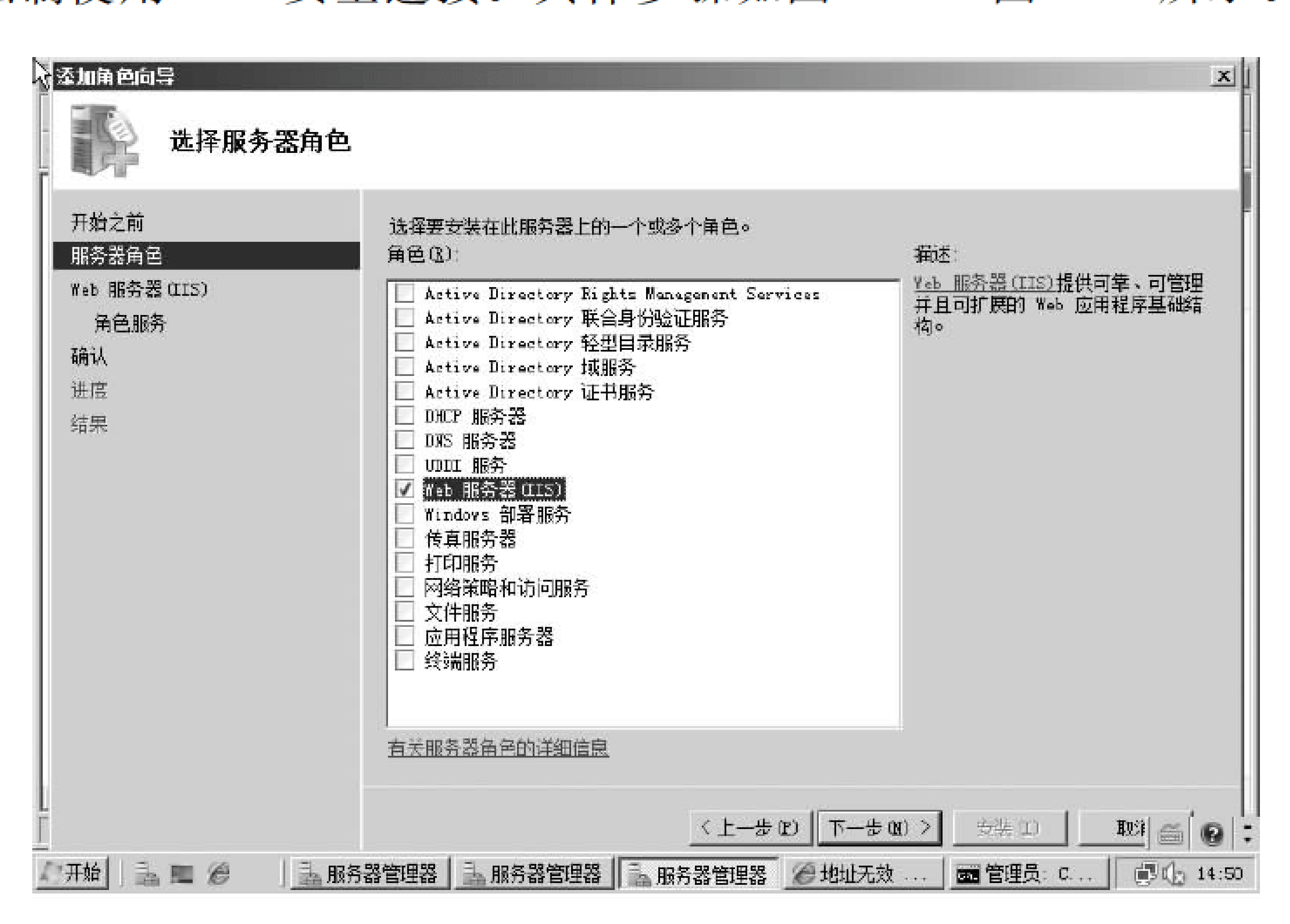


图 6-28　添加 IIS 服务



图 6-29　启动 IIS 服务



图 6-30　在 IIS 服务中选择服务器证书



图 6-31　选择创建证书申请

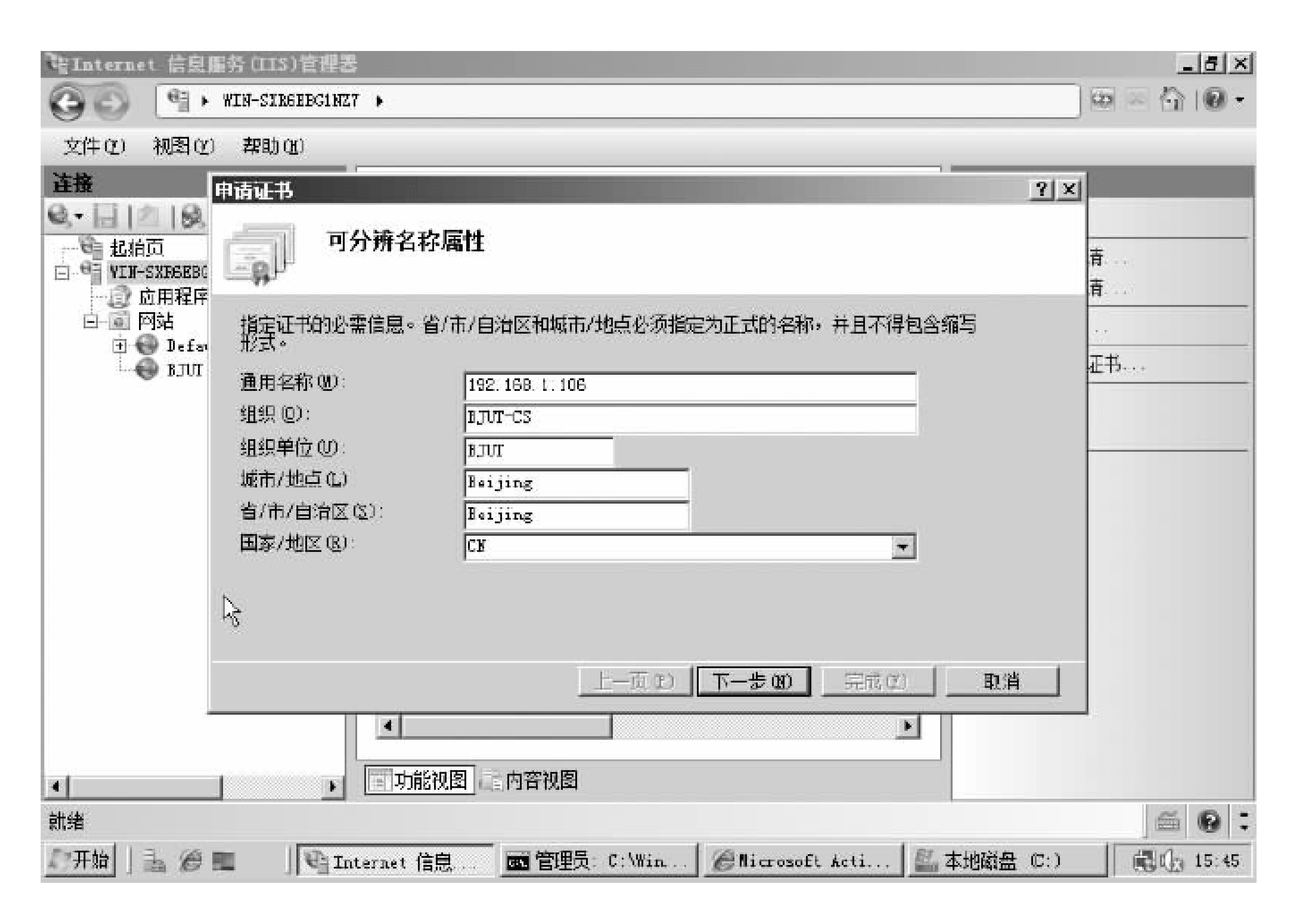


图 6-32　填写证书申请



图 6-33 选择加密程序



图 6-34 存放证书申请

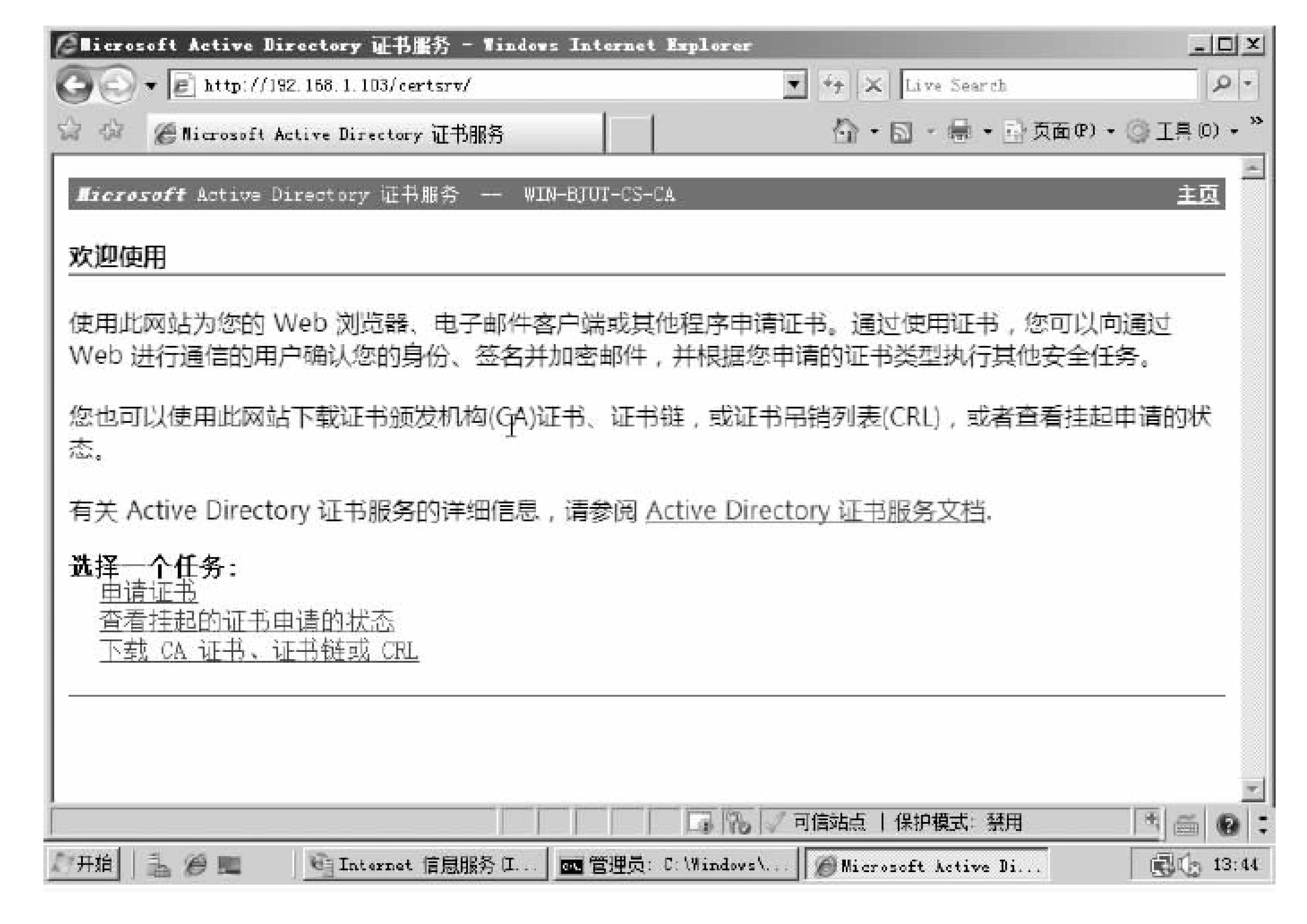


图 6-35 打开证书申请页面



图 6-36　选择高级证书申请



图 6-37　选择使用 base64 编码的 CMC 或 PKCS＃10 文件提交一个证书申请



图 6-38　复制事先存放的证书申请



图 6-39 填写证书申请

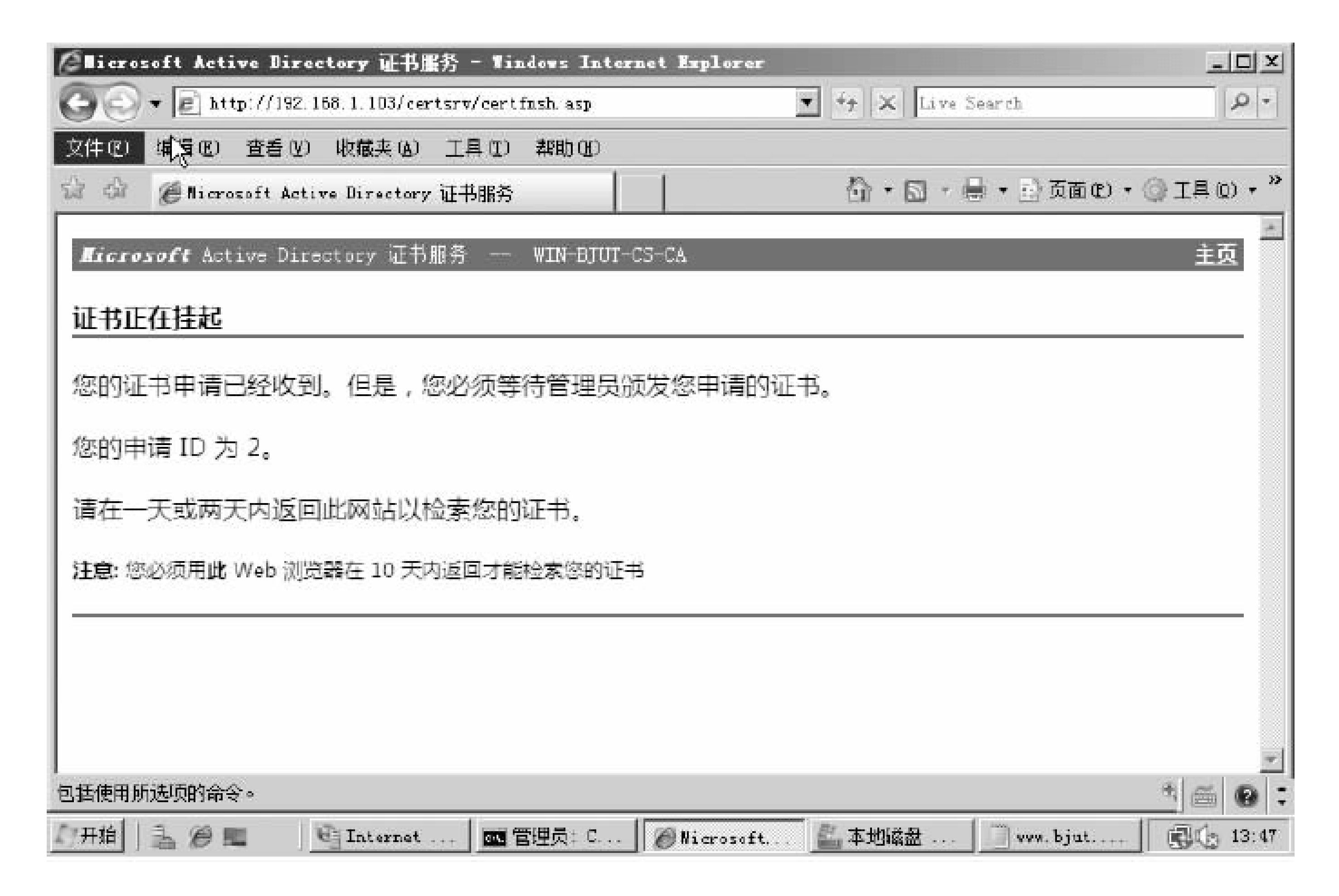


图 6-40 提交证书申请



图 6-41 证书服务器批准证书申请



图 6-42 Web 服务器下载证书



图 6-43 为 Web 服务器完成证书申请



图 6-44 Web 服务器完成证书申请

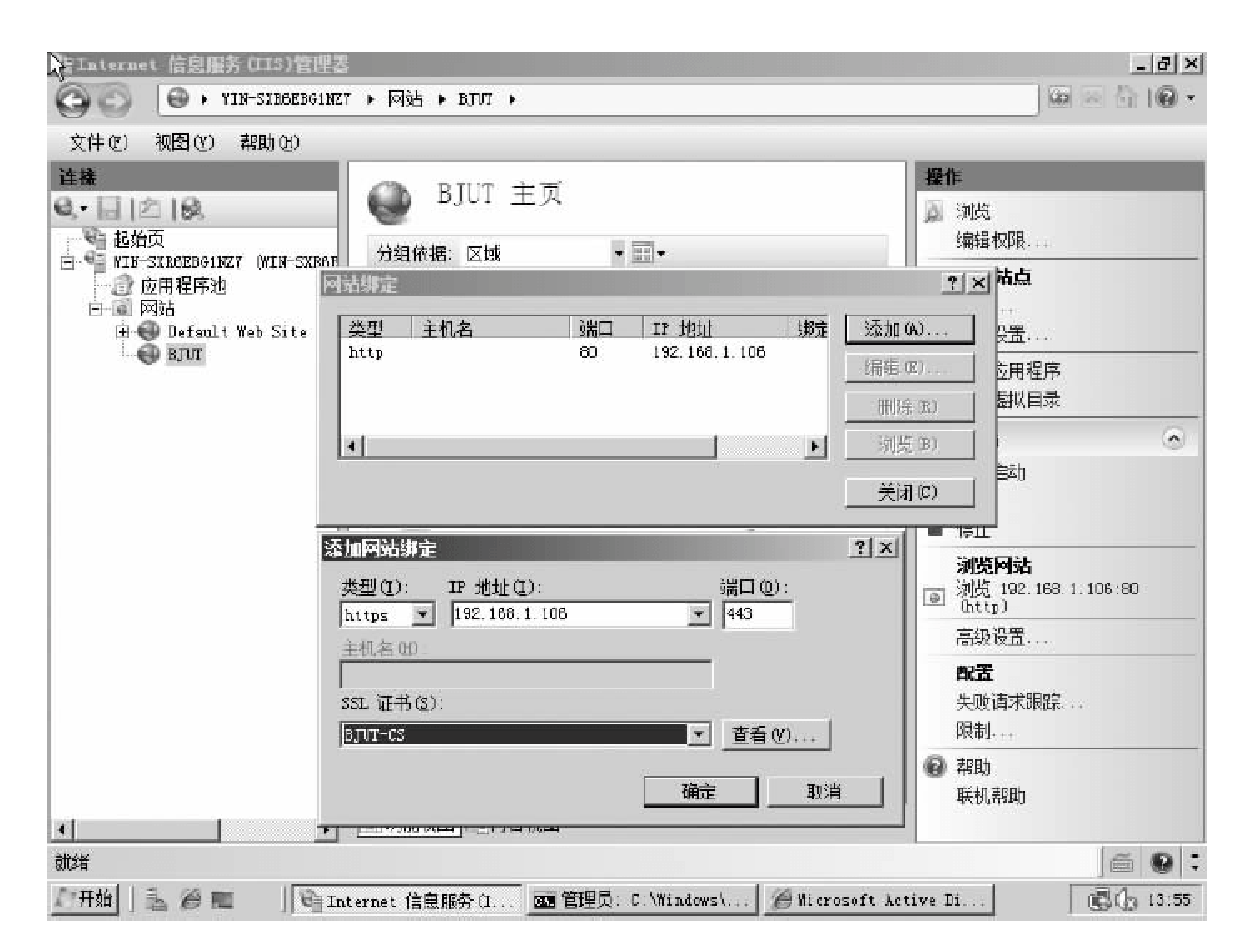


图 6-45　Web 网站添加一个 HTTPS 类型并选择证书



图 6-46　为 Web 网站设置使用 SSL

3. 客户端证书申请与配置

(1) 客户端访问 Web 服务器站点。站点要求证书验证，单击继续浏览，查看证书，提示“无法将这个证书验证到一个受信任的证书颁发机构”。

(2) 下载 CA 证书。浏览器地址栏中输入“http://证书服务器地址/certsrv/”，打开证书服务界面。下载 CA 证书，并将其安装到受信任的根证书颁发机构。

(3) 客户端再次访问 Web 服务器站点，在访问通过 SSL 加密的站点时所输入的地址应该以 https://开头，如果仍然使用 http://则会出现错误提示。地址栏能正常显示安全挂锁标志，标志客户端和服务器之间成功通过 SSL 加密信道进行通信。

具体步骤如图 6-47～图 6-52 所示。



图 6-47　用 HTTP 协议访问 Web 服务器站点失败

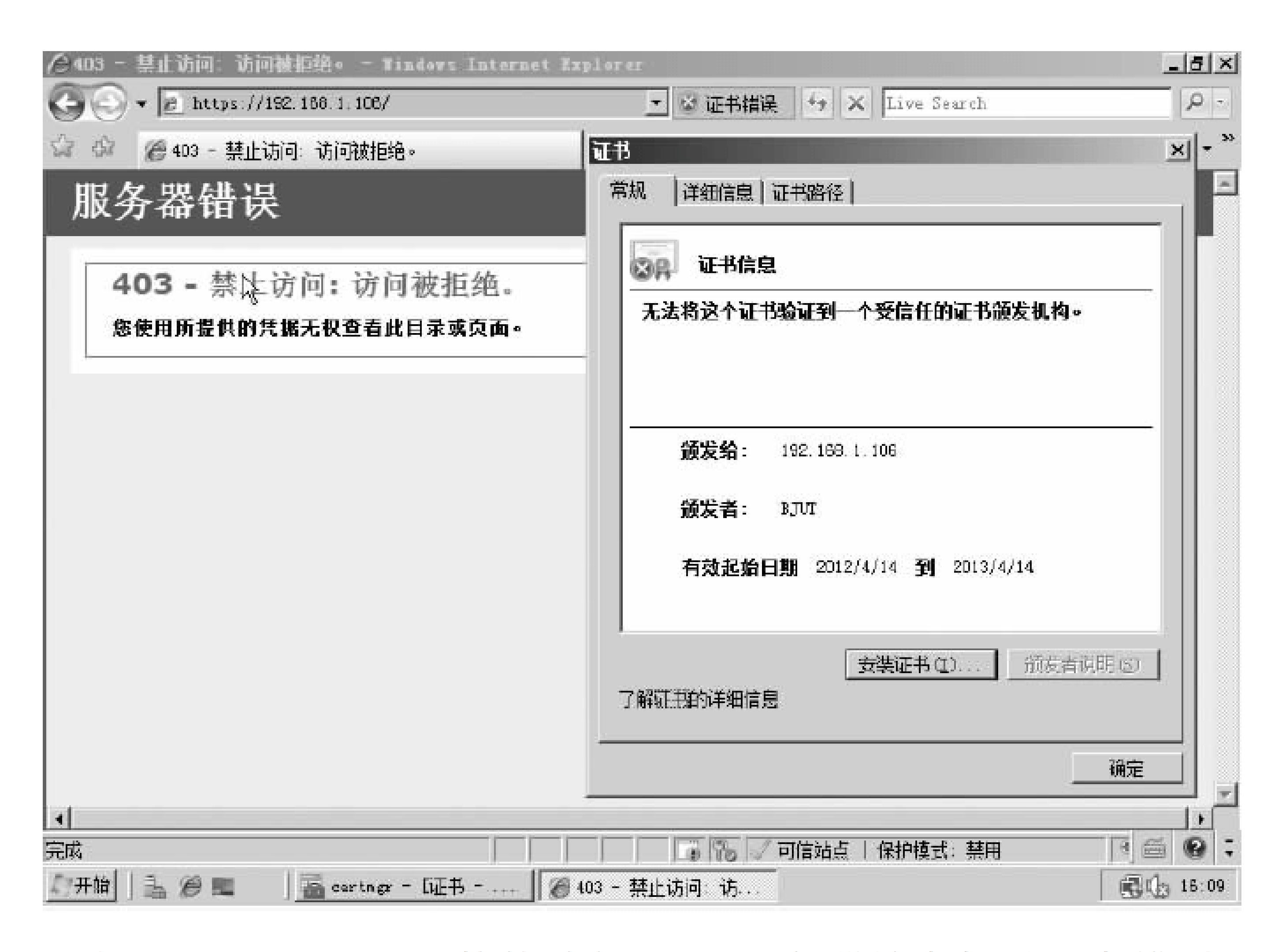


图 6-48　用 HTTPS 协议访问 Web 服务器站点提示证书错误

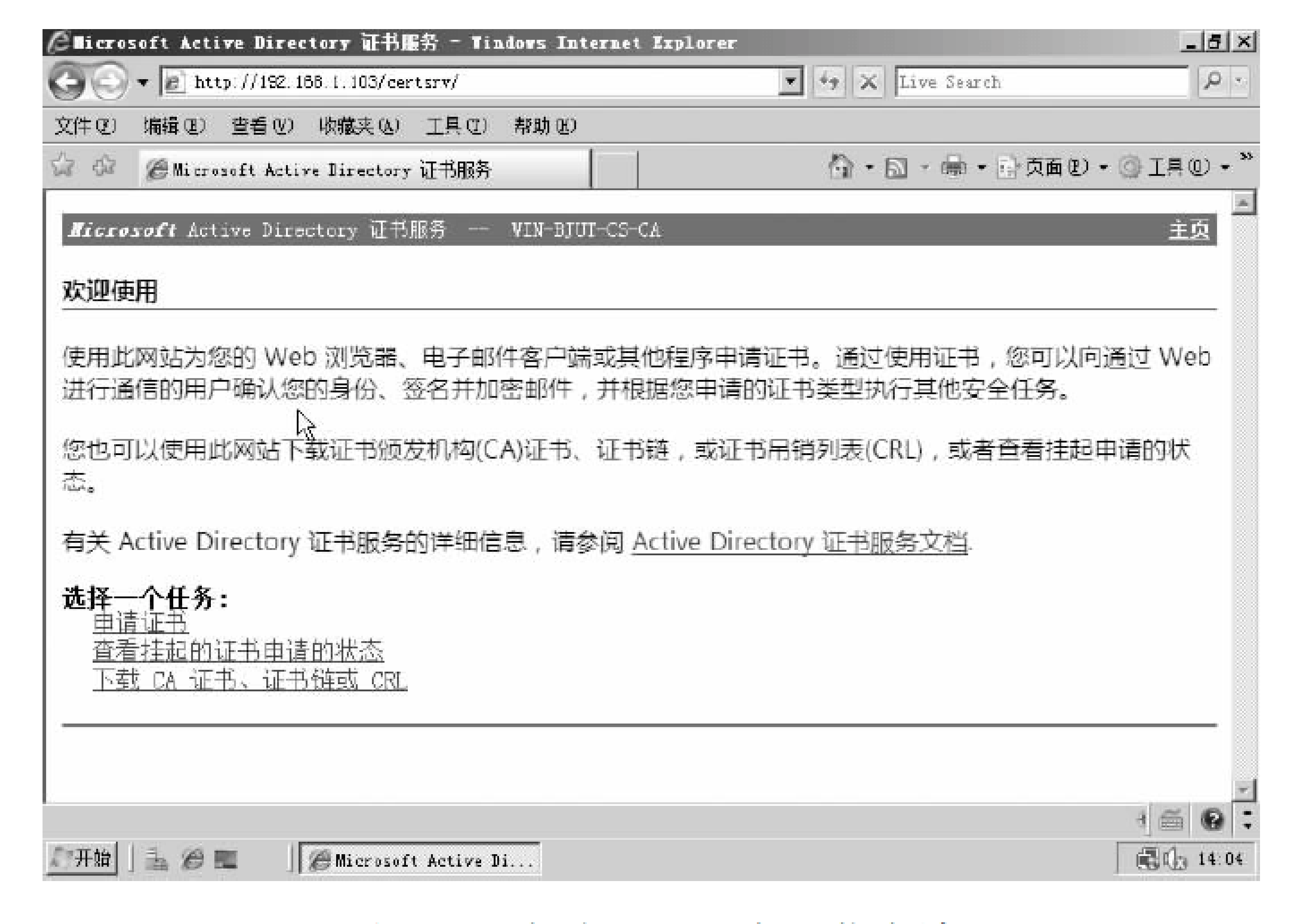


图 6-49　提交 CA 证书下载申请

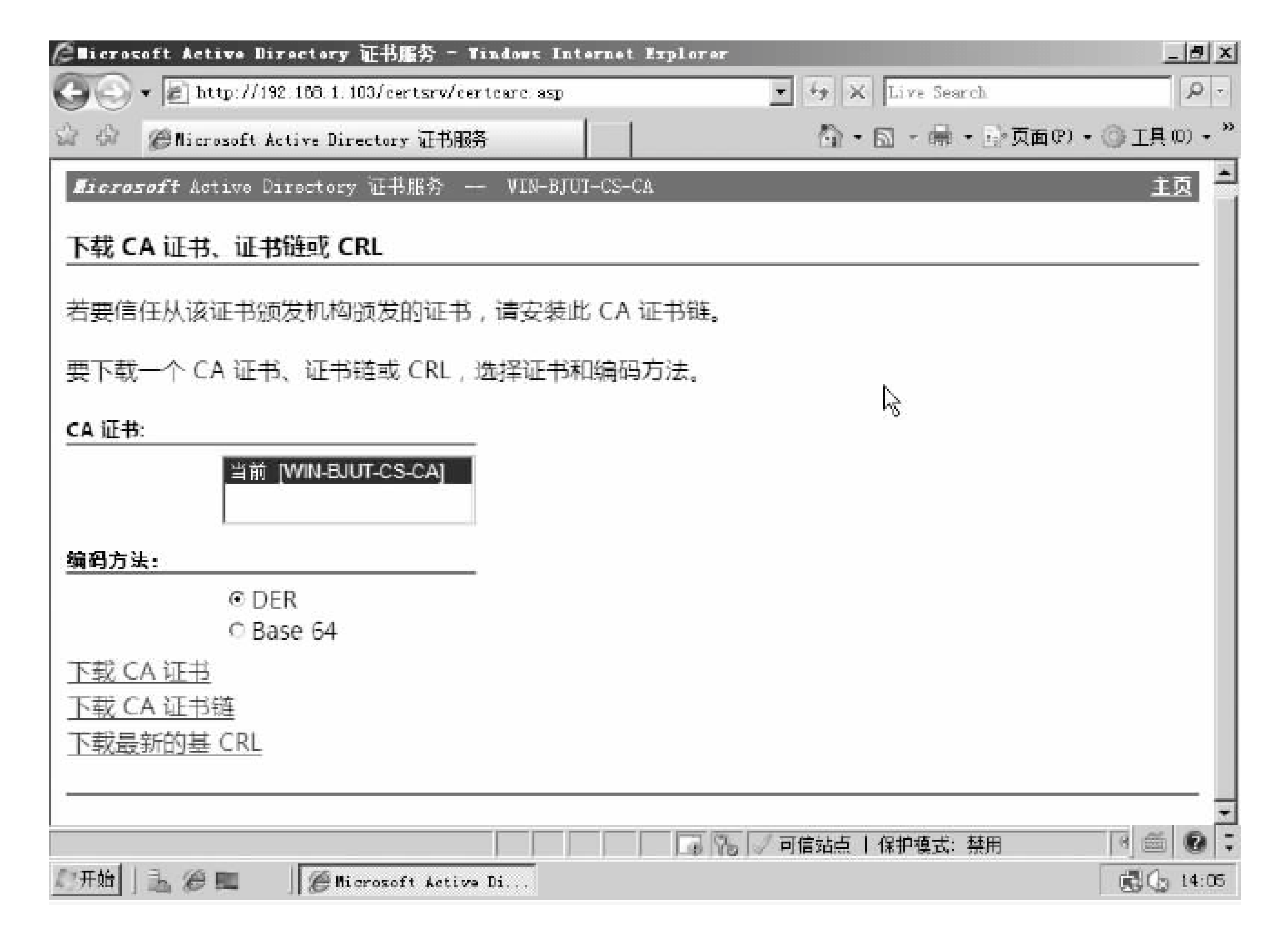


图 6-50 Web 服务器下载 CA 证书

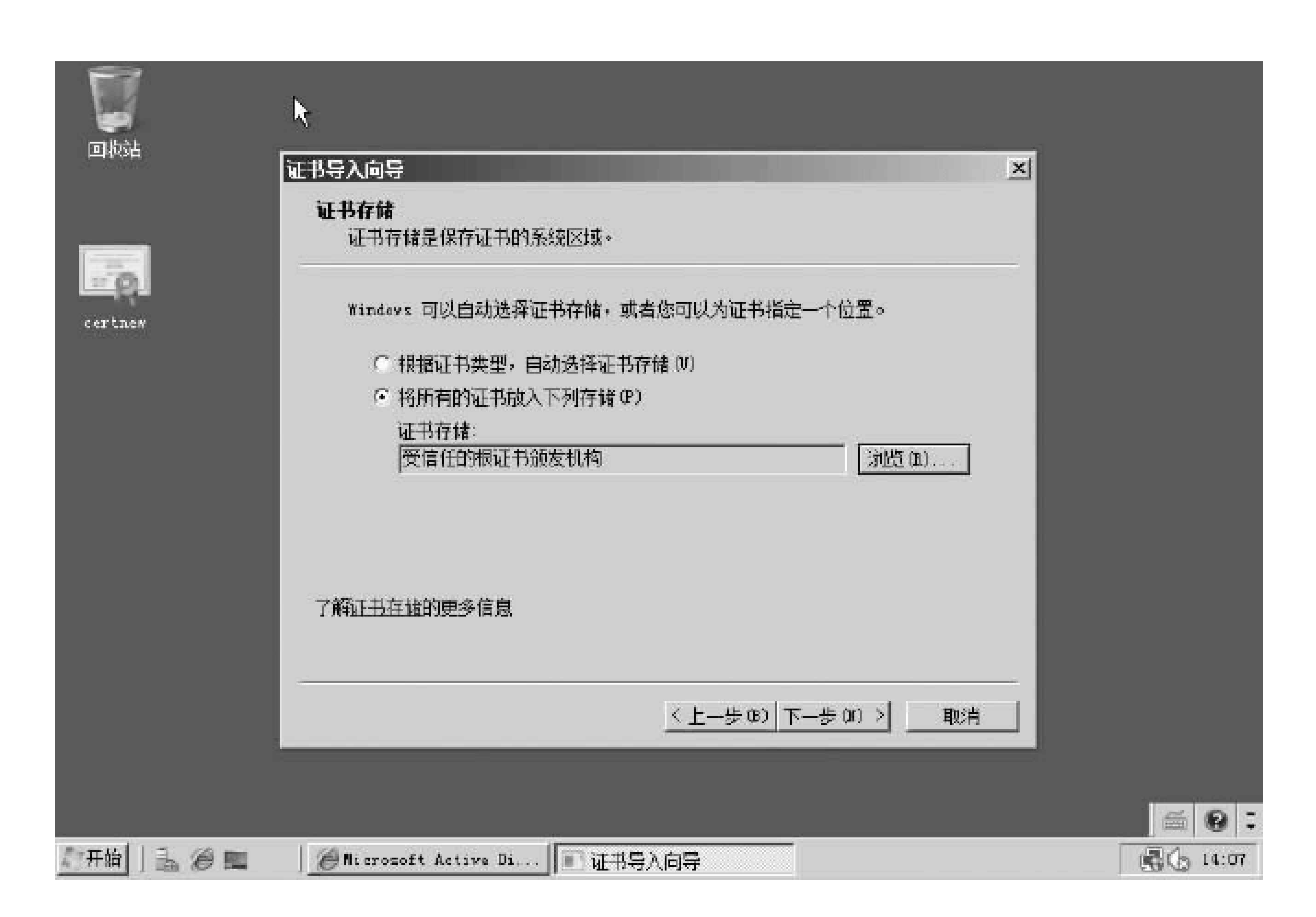


图 6-51 安装 CA 证书到受信任的根证书颁发机构



图 6-52 通过 SSL 加密通道正常访问站点

习题 6

1. 简述应用层的安全威胁，并结合身边的情况给出实例。

2. 假设邮件系统使用 SMTP 和 POP3 进行 E-mail 的发送和接收，说明电子邮件的传输过程，并分析其薄弱环节，探讨可能的解决方案。

3. 通过调研说明如何通过设置常见的邮件客户端（如 Outlook、Foxmail 等）实现邮件加密、数字签名、垃圾邮件过滤功能。

4. 加密和解密过程需要耗费系统大量的资源。如果网站所有的 Web 应用数据都使用 S-HTTP 协议加密传输，将严重降低系统的效率。能否在保证应用安全的前提下，对应用数据进行区分传输，对敏感数据使用 S-HTTP 安全通道传输，而对非敏感数据只进行 HTTP 非安全通道传输？试举出 3 种可能的区分原则和实例。

5. 不同应用因特性和场景的不同，会面临不同的安全威胁。那么应该为不同的应用设计相应的个性化安全增强方法，还是应该根据不同应用面临安全风险的共性开放通用安全增强方法？请给出选择并说明原因，同时通过调研说明现实情况。

第 7 章　VPN 基础

随着企业信息化和电子商务的迅猛发展，企业规模越来越大，所跨地域越来越广，合作伙伴越来越多，传统企业网基于固定物理地点的专线或虚拟专线的连接方式，已难以适应现代企业发展的需求。企业用户已经不仅仅满足于基本的网络互联能力，而在网络的灵活性、安全性、经济性和可扩展性等方面都提出了更高要求。如果采用传统的租用专线，虽然在安全性方面有足够的保证，但是仍不能从根本上解决企业用户的实际困难。在这样的背景下，一种基于公用网络的动态、安全的连接解决方案就成为时代之需，VPN 技术就是这样一种网络连接技术。

VPN 可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。通过将数据流转移到低成本的虚拟专用网络上，一个企业的虚拟专用网解决方案将大幅度减少用户花费在城域网和远程网络连接上的费用。同时，还将简化网络的设计和管理，加速连接新的用户和网站。另外，VPN 还可以保护现有的网络投资。随着用户的商业服务不断发展，企业的 VPN 解决方案可以使用户将精力集中到自己的生意上，而不是网络上。VPN 可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济有效地连接到商业伙伴和用户的安全外联网 VPN。

7.1　VPN 概念

自从出现了 Internet，网络管理员一直在寻找利用这个廉价且被广泛使用的媒介来传输数据的方法，并且能同时保护数据的完整性和机密性；既能保护分组中信息，又能为终端用户提供透明传输的方法，这便促成了虚拟专用网（Virtual Private Networks，VPN）概念的产生。

Virtual，是针对传统的企业“专用网络”而言的。传统的专用网络往往需要建立自己的物理专用线路，使用昂贵的长途拨号以及长途专线服务；而 VPN 则是利用公共网络资源和设备，建立一个逻辑上的专用通道，尽管没有自己的专用线路，但是这个逻辑上的专用通道却可以提供和专用网络同样的功能。换言之，VPN 虽然不是物理上真正的专用网络，但却能够实现物理专用网络的功能。

Private，表示 VPN 是被特定企业或用户私有的，并不是任何公共网络上的用户都能够使用已经建立的 VPN 通道，而只有经过授权的用户才可以使用。在该通道内传输的数据经过了加密和认证，使得通信内容既不能被第三者修改，又无法被第三者破解，从而保证了传输内容的完整性和机密性。因此，只有特定的企业和用户群体才能利用该通道进行安全的通信。

Network，表示这是一种专门的组网技术和服务，企业为了建立和使用 VPN，必须购

买和配备相应的网络设备。

综上所述，虚拟专用网(VPN)定义为利用共享的公用网络建立特定用户的数据传输通道，将企业用户的远程分支办公室、商业合作伙伴、移动办公人员等连接起来，提供端到端的、有一定安全和服务质量保证的数据通信服务的网络技术。虚拟专用网是对企业内部网的扩展，为了保障信息的安全，VPN 技术采用了鉴别、访问控制、保密性、完整性等措施，以防止信息被泄露、篡改和复制。

7.2 VPN 的工作原理

在 VPN 定义的基础上来分析一下 VPN 的原理。一般来说，两台具有独立 IP 并连接上互联网的计算机，只要知道对方的 IP 地址，就可以进行直接通信。但是，位于这两台计算机之下的内部私有网络是不能直接互连的，原因是私有网络通常使用保留地址作为内部 IP，这些保留地址在 Internet 上是无法被路由的，所以正常情况下无法直接通过 Internet 访问到局域网内的主机。VPN 的原理就是在这两台直接和公网连接的计算机之间建立一条专用通道。为了实现这一目的，需要使用 VPN 隧道技术，VPN 的工作原理如图 7-1 所示。

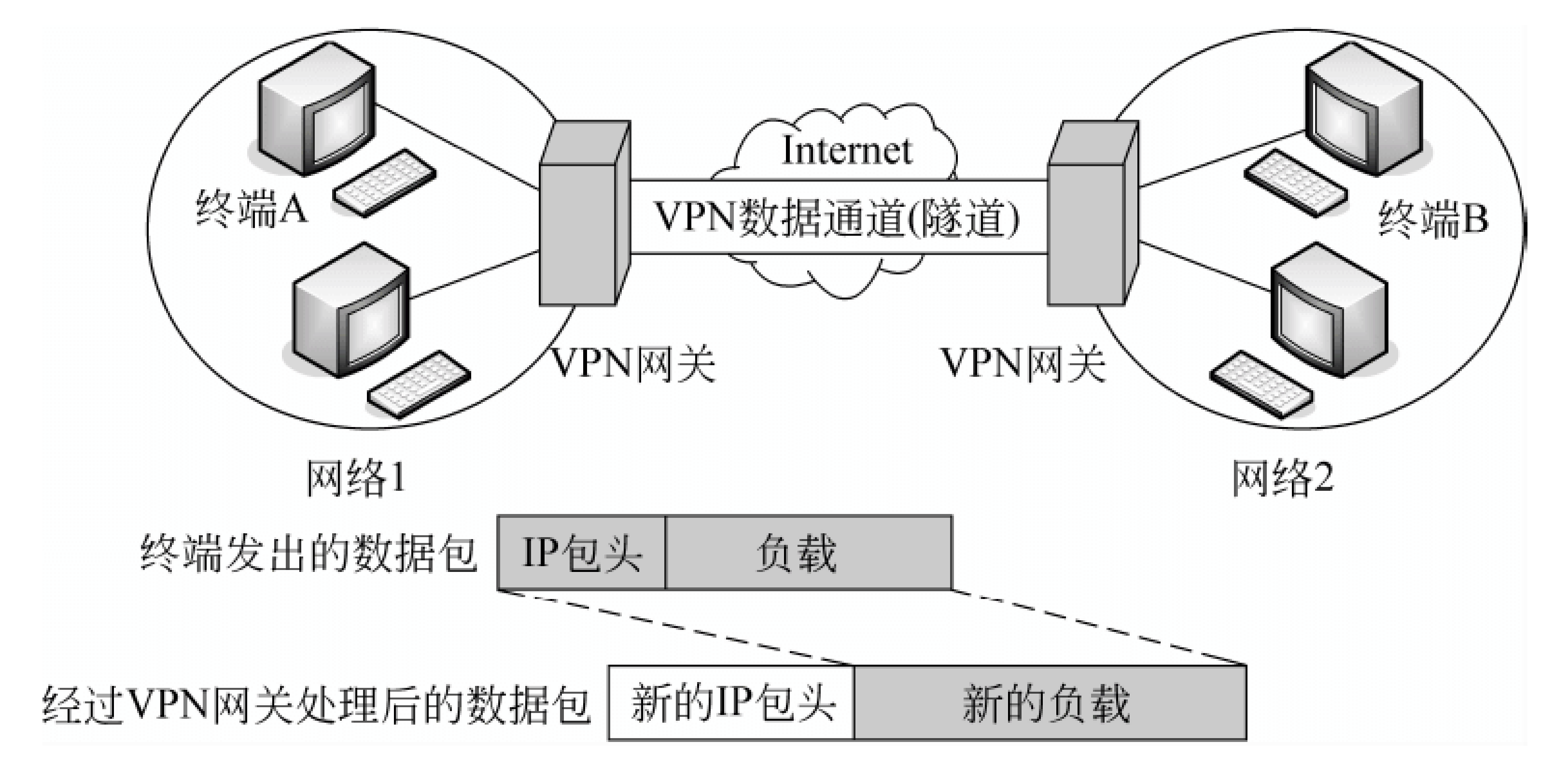


图 7-1 VPN 的工作原理

通常情况下，VPN 网关采用双网卡结构，外网卡使用公共 IP 接入 Internet。

如果网络 1 的终端 A 需要访问网络 2 的终端 B，其发出的访问数据包目标地址为终端 B 的 IP (内部 IP)。

网络 1 的 VPN 网关接收到终端 A 发出的访问数据包时，对其目标地址进行检查，如果目标地址属于网络 2 的地址，则向网络 2 的 VPN 网关发出连接请求；网络 2 的 VPN 网关响应请求，并向网络 1 的 VPN 网关发出身份质询，网络 1 的 VPN 网关将加密的用户身份验证响应信息发送到网络 2 的 VPN 网关；网络 2 的 VPN 网关根据用户数据库检查该响应，如果账户有效，将检查该用户是否具有远程访问权限；如果该用户拥有远程访问的权限，网络 2VPN 网关接受此连接。

网络 1 的 VPN 网关将该数据包进行封装、加密，封装的方式根据所采用的 VPN 技术不同而不同，同时 VPN 网关会构造一个新的数据包(VPN 数据包)，并将封装后的原

数据包作为 VPN 数据包的负载,在身份验证过程中产生的公有密钥将用来对数据进行加密,VPN 数据包的目标地址为网络 2 的 VPN 网关的外部地址。

网络 1 的 VPN 网关将 VPN 数据包发送到 Internet,由于 VPN 数据包的目标地址是网络 2 的 VPN 网关的外部地址,所以该数据包将被 Internet 中的路由正确地发送到网络 2 的 VPN 网关。

网络 2 的 VPN 网关对接收到的数据包进行检查,如果发现该数据包是从网络 1 的 VPN 网关发出的,即可判定该数据包为 VPN 数据包,并对该数据包进行解包处理。解包的过程主要是先将 VPN 数据包的包头剥离,再通过 VPN 技术将负载反向处理还原成原始的数据包。

网络 2 的 VPN 网关将还原后的原始数据包发送至目标终端,由于原始数据包的目标地址是终端 B 的 IP,所以该数据包能被正确地发送到终端 B。在终端 B 看来,它收到的数据包就像从终端 A 直接发过来的一样。

从终端 B 返回终端 A 的数据包处理过程与上述过程一样,这样两个网络内的终端就可以相互通信了。

通过上述说明可以发现,在 VPN 网关对数据包进行处理时,有两个参数对于 VPN 隧道通信十分重要:原始数据包的目标地址(VPN 目标地址)和远程 VPN 网关地址。根据 VPN 目标地址,VPN 网关能够判断对哪些数据包需要进行 VPN 处理,对于不需要处理的数据包,通常情况下可直接转发到上级路由;远程 VPN 网关地址则指定了处理后的 VPN 数据包发送的目标地址,即 VPN 隧道的另一端 VPN 网关地址。由于网络通信是双向的,在进行 VPN 通信时,隧道两端的 VPN 网关都必须知道 VPN 目标地址和与此对应的远端 VPN 网关地址。

由于 VPN 连接的特点,私有网络的通信内容会在公用网络上传输,出于安全和效率的考虑,通信内容需要加密或压缩。而通信过程的打包和解包工作则必须通过一个双方协商好的协议进行,这样,在两个私有网络之间建立 VPN 通道将需要一个专门的过程,依赖于一系列不同的协议。这些设备和相关的设备及协议组成了一个 VPN 系统。

VPN 数据通道(隧道)是由隧道协议形成的。数据包通过 VPN 隧道协议封装、加密、传输到目的内部网络。Internet 工程任务组(Internet Engineering Task Force,IETF)负责定义协议和规章,所有 VPN 提供商均使用这些协议和规章,以保护数据机密性。这些协议包括点对点隧道协议(Point to Point Tunneling Protocol,PPTP)、第 2 层转发(Layer 2 Forwarding,L2F)、第 2 层隧道协议(Layer 2 Tunneling Protocol,L2TP)、通用路由选择封装(Generic Routing Encapsulation,GRE)、多协议标记交换(Multiprotocol Label Switching,MPLS)VPN、Internet 协议安全(Internet Protocol Security,IPSec)和安全套接字层 VPN(SSL VPN)等。

7.3 VPN 的特点

在实际应用中,一个高效、成功的 VPN 应具备以下 5 个主要特点。

1. 具备完善的安全保障机制

传统 Internet 方式由于透过公众网络传输资料,因此在资料的安全性上无法得到保

障，更无法达到ERP、BOSS系统对安全性的要求。

VPN方式则会在公众网络上建立一个逻辑的、点对点的连接，称为建立一个隧道，并利用加密技术，对经过隧道传输的数据进行加密，以保证数据仅被指定的发送者和接收者了解，从而保证了数据的私有性和安全性。

2. 具备用户可接受的服务质量保障

广域网流量的不确定性使透过公众网络传输数据时的带宽利用率很低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不到及时发送；而在流量低谷时，又造成大量的网络带宽空闲。

VPN方式通过流量预测与流量控制策略，可以按照优先级分配带宽资源，实现带宽管理，使各类数据能够被合理地先后发送，并预防阻塞的发生。

3. 具备灵活的可扩充性

传统长途专线方式每增加一个点，都需要在该点和其他所有要连接的点之间增加多条物理线路投入、终端设备的投入，对已有每个点的设备进行升级，以满足端口增加的需求。

采用VPN方式，用户只要接入新的结点，并提供新点与其他点之间的通信规则，就无须考虑其他结点设备上的预留。

4. 管理便捷

在传统方式下，企业无法将网络管理功能从局域网无缝延伸到公用网，甚至是客户和合作伙伴。

VPN方式运营商可协助用户规划管理整个网络，降低了对用户自身IT技术管理的要求。而MPLS VPN产品，更因为支持使用私有地址，对于那些已有局域网且已做私有地址规划的用户有巨大吸引力。客户不必改变原有IP地址规划方案，且可以有效保护用户在设备上的投资。

5. 节省成本

传统长途专线方式成本巨大，且每新增一点，需要新增N－1条线路（N＝该企业所有点数），所需费用将呈几何级数增长。

采用VPN方式时，增加新的结点，用户只要接入新的结点，并提供新点与其他点之间的通信规则，费用相对低廉很多。

7.4 VPN的分类

VPN技术虽然出现的时间不长，但由于具有突出的优越性，在较短时间内得到了广大企业用户的青睐，这又推动了VPN技术的迅速发展。目前，各种各样的VPN技术层出不穷，根据不同的划分标准，可以把VPN划分为多种类型。

(1) 根据所利用的公共主干网是否是 IP 网,VPN 分为两种情况。

① Non-IP VPN。可以是指传统意义上的 VPN,也就是在分组交换网(PAC)、数据数字网(DDN)或帧中继网(FRN)上组建 VPN,即利用数据数字网、公用分组交换网或帧中继网的部分网络资源,如传输线路、网络模块、网络端口等划分成一个分区,并设置相对独立的网络管理机构,对分区内数据量及各种资源进行管理,分区内的各结点共享分区内的网络资源,它们之间的数据处理和传送相对独立,就好像真正的专用网一样。

或者是指支持 MPLS、IPX 等非 IP 协议网络的 VPN。

② IP VPN。依靠 ISP 和其他 NSP(网络服务提供商),在 IP 网络(包括公用的 Internet 或专用的 IP 骨干网等)中建立专用的数据通信网络的技术。更准确地讲,RFC 2764 对 IP VPN 的阐述是"IP VPN 是指使用 IP 网络设施对专用广域网的仿真"。

(2) 根据接入方式不同,可划分为两种情况。

① 专线 VPN。为已经通过专线接入 ISP 边缘路由器的用户提供的 VPN 实现方案。典型的专线方式有租用线、以太网、VLAN、ATM、帧中继等。

采用专线方式设备成本较高,且设备配置比较复杂,因此站点之间不使用全网状连接,而采用某些形式的层次化结构。专线方式一般用于 LAN 之间的连接,或者计算机之间的连接。专线方式经历了一个不断发展完善的过程。从最初的物理专线(物理层)方式,发展到逻辑专线(链路层)方式,再发展到今天的基于因特网协议(IP)的 IP 逻辑专线,甚至基于 IP 的逻辑专网方式。

② 拨号 VPN(VPDN)。指为利用拨号方式接入 ISP 的用户提供的 VPN 业务。典型的拨号方式有公众交换电话网(PSTN)、综合业务数字网(ISDN)、蜂窝移动通信网(PLMN)、数字用户线路(xDSL)、有线电缆调制解调和无线移动接入等。主要是基于 PPTP 和 L2F 协议。

一般而言,拨号方式是通过在一个或多个中心站点部署接入服务器(NAS)来实现的。用户(计算机)首先拨号接入某个 NAS,该 NAS 与认证、授权和计费(AAA)服务器交互,验证用户身份,并根据验证结果授权使用站点中的某些资源和服务。

拨号方式一般用于计算机与 LAN 之间或计算机与计算机之间的连接。

专线接入与拨号接入之间的最大区别是拨号接入是"按需"接入的,一般每次接入都需要做认证;而专线接入一般是"永远在线"的,不需要每次接入都做认证,有时甚至连认证的必要都没有。

(3) 根据 VPN 实现方式的不同,可划分为 3 种情况。

① 软件 VPN。利用软件公司提供的完全基于软件的 VPN 产品来实现的 VPN。当对数据连接速率要求不高,对性能和安全性要求不强时,可以利用完全基于软件的 VPN 产品来实现简单的 VPN 功能,如 Checkpoint Software 和 Aventail Corp 等公司的产品。甚至可以不需要另外购置软件,仅依靠微软公司的 Windows 操作系统,特别是自 Windows 2000 版本以后的系统,就可实现纯软件平台的 VPN 连接。

这类 VPN 网络的性能一般较差,数据传输速率较低,同时安全性也较低,一般仅适用于连接用户较少的小型企业。

② 硬件 VPN。利用硬件厂商提供的专用硬件平台来实现的 VPN。使用专用硬件平

台的 VPN 设备，可以满足企业和个人用户对高数据安全及通信性能的需求，尤其是实现从加密及数据乱码等对 CPU 处理能力需求很高的功能。提供这些平台的硬件厂商比较多，比较有名的如国外的 Norvel、Array Networks、Cisco、3Com 等，国内的如华为、联想等。

这类 VPN 平台虽然投入了大量的硬件设备，但是具有先天的不足，就是成本太高，中、小型企业很难承受。由于全是由硬件构成的平台，因此在管理的灵活性和可管理性方面就显得不如人意。通常，对于专业的 VPN 网络服务提供商来说较为合适，因为它们都有这方面的人才和资金优势。不过现在的主流 VPN 硬件设备制造商都能提供相应的管理软件来支持，如 Cisco、3Com 公司等。

③ 辅助硬件 VPN。辅助硬件平台的 VPN 主要是指以现有网络设备为基础、再增添适当的 VPN 软件实现的 VPN。这类 VPN 平台介于软件平台和指定硬件平台之间，是一种最常见的 VPN 平台，也是性能最好的一种。但是，通常这种平台中的硬件也不能完全由原来的网络硬件组成，必要时还要添加专业的 VPN 设备，如 VPN 交换机、VPN 网关或路由器等，这对一个完善的、高性能的 VPN 网络设备是非常必要的。

这种平台是最为通用的一种方式，它既具备了硬件平台的高性能、高安全性，也具有软件平台的灵活性，并且可以利用绝大多数现有硬件设备，节省了总体投资。目前，绝大多数企业的 VPN 方案选用这种方式。

（4）根据运营商所开展的业务类型，可划分为 4 种情况。

① 拨号 VPN 业务。实际上是根据接入方式划分的 VPDN。

② 虚拟租用线（VLL）。它是对传统租用线业务的仿真，用 IP 网络对租用线进行模拟，在两端的用户看来，这样一条虚拟租用线等价于过去的租用线。

③ 虚拟专用路由网（VPRN）业务。VPRN 是对三层 IP 路由网络的一种仿真，利用公共 IP 网络，在多个 VPN 成员之间建立起一个虚拟的隧道网络。

④ 虚拟专用局域网段（VPLS）。VPLS 利用互联网络设施仿真局域网段，转发表中包含介质访问控制层的可达信息。

（5）根据路由管理方式，可划分为两种情况。

① 叠加模式（Overlay Model）。也译为“覆盖模式”。目前，大多数常用的 VPN 技术都基于叠加模式，如 IPSec、GRE 等隧道技术、租赁线路、帧中继电路、ATM 电路等。采用叠加模式，各站点都有一个路由器，通过点对点连接到其他站点的路由器上。一个站点可以有一个或多个这样的路由器，分别连接到所有或一部分其他站点上；站点间点对点的连接可以通过 IPSec、GRE 或帧中继、ATM 电路等来实现。这个由点对点的连接以及相关路由器组成的网络为“虚拟骨干网”。虚拟骨干网将各站点连接在一起。

叠加模式的一个严重问题是需要 VPN 用户来设计并运作虚拟骨干网。这需要专业的 IP 路由知识和技能，而大多数公司不具备这样的能力。如果将这项工作交给网络服务提供商，随着 VPN 用户的增加，网络服务提供商需设计维护越来越多的 VPN，这对网络服务提供商来说难以承受。

叠加模式的另一个问题是 VPN 的网络规模不能太大，可扩展性差。如果一个 VPN 用户有许多站点，而且站点间需要全交叉网状连接，则一个站点上的骨干路由器必须与其

他所有站点建立点对点的路由关系。站点数的增加受到单个路由器处理能力的限制。另外,增加新站点时,网络配置变化也会很大,网状连接上的每一个站点都必须对路由器重新配置。

② 对等模式(Peer Model)。对等模式是针对叠加模式固有的缺点推出的,实现了用户路由的动态发布。它通过限制路由信息的传播来实现 VPN,这种模式能够支持大规模的 VPN 业务,如一个 VPN 服务提供商可支持成百上千个 VPN。采用这种模式,相关的路由设备很复杂,但实际配置却非常简单;容易实现 QoS 服务;扩展更加方便,新增一个站点,不需与其他站点建立连接就能实现和其他所有分支结点的通信。这对于网状结构的大型复杂网络非常有用。典型代表包括在共享路由器上配置严格的访问列表、使用虚拟专用路由器、使用三层 MPLS VPN 技术组网等。

(6) 根据实现方式,可划分为两种情况。

① 用户管理的 VPN (CPE-VPN)。CPE-VPN 是用户自己设置、管理并维护 VPN 网关设备。通过公共 IP 网,在各个分支机构和公司总部之间建立基于标准 VPN 隧道的连接,隧道协议通常采用二层隧道协议 (L2TP)、点对点隧道协议(PPTP)、IPSec、IP in IP 和通用路由选择封装(GRE)等,并且利用各种加密技术和网络地址转换(NAT)技术来保障数据传输的安全。VPN 隧道连接的建立与管理完全由用户自己负责,提供商不需要调整或改变网络的结构与性能。这种方式也就是通常所说的"自建 VPN"方式。

② 提供商实施的 VPN (PP-VPN)。PP-VPN 是指在提供商的公共数据网上设置 VPN 网关设备,用于专线接入用户或远程拨号接入用户。利用该网关设备,可以在全网范围内,根据具体的 VPN 网络需求,通过隧道封装、虚拟路由器或 MPLS 等技术建立 VPN,并且可以采用加密技术,以保障数据传输的安全。VPN 连接的建立完全由提供商负责,对用户透明。这种方式也就是通常所说的"外包 VPN"方式。

7.5 VPN 应用领域

VPN 应用领域可分为如下 3 个方面。

7.5.1 企业内部虚拟网

企业内部网的 VPN 建立在集团总部与远程销售分部之间,或集团总部与通过卫星通信的远程办事处之间。企业内部网的 VPN 可以在公司网络内部使用,仅能被公司员工访问;也可以从外部访问,仅能被公司有权限的员工访问。图 7-2 描述了一种典型的企业内部网服务方式。

随着企业的跨地区以及经营国际化,绝大多数大、中型企业都要求对企业内部各分支机构进行互联。各分公司之间传统的网络连接方式一般是租用专线。显然,在分公司增多、业务范围越来越广时,网络结构会变得越来越复杂,费用也会越来越昂贵。利用 VPN 特性,可以在 Internet 上组建世界范围内的 Intranet VPN,企业内部网能够实现站点到站点的连接。利用 Internet 的线路,可以保证网络的互联性,利用隧道、加密等 VPN 特

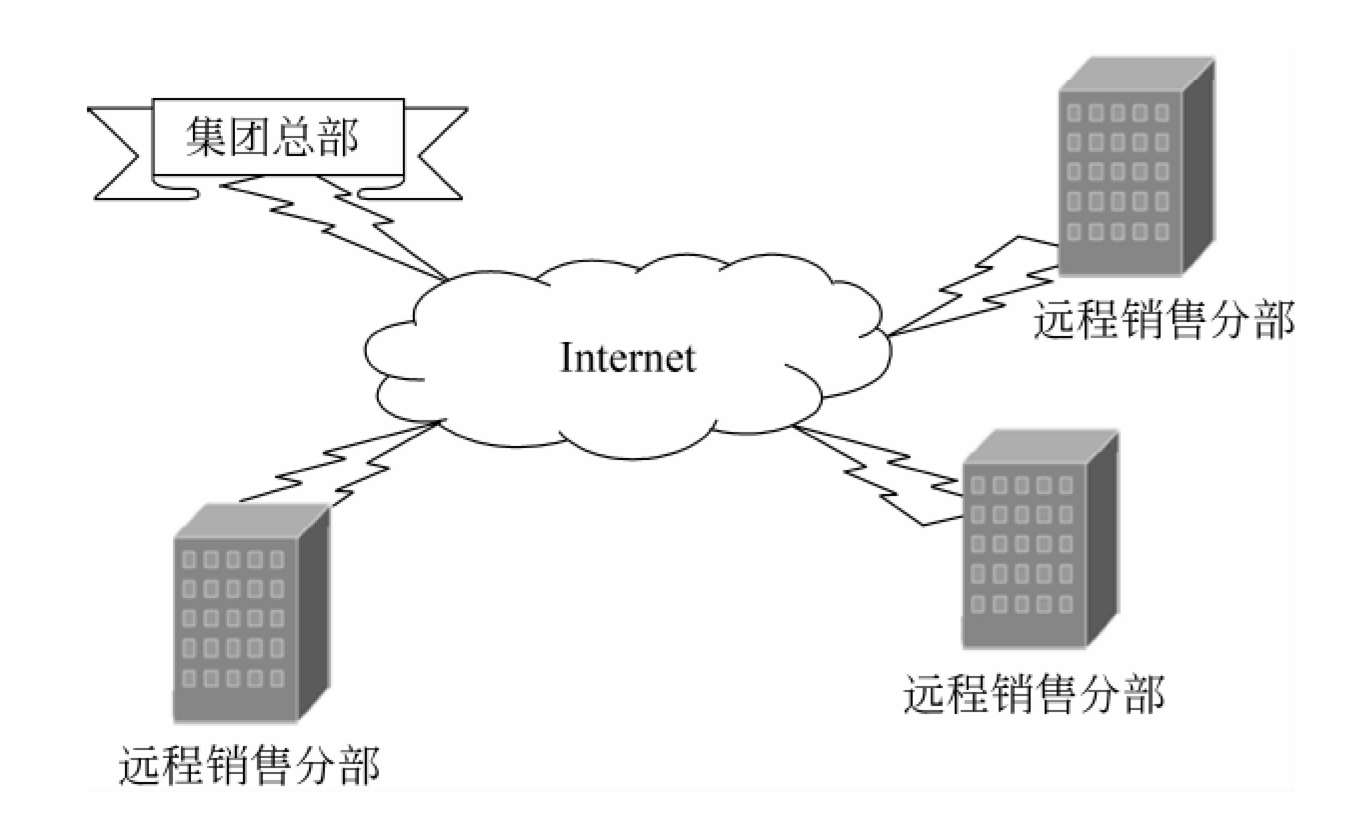


图 7-2　企业内部互联的 VPN

性，可以保证信息在整个 Intranet VPN 上安全传输。Intranet VPN 通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络相同的政策，包括安全、服务质量(QoS)、可管理性和可靠性。

按照企业的不同需求以及组网要求，可以灵活地规划不同的 Intranet VPN 组网方式。Intranet VPN 逻辑连接的拓扑类型主要有星状连接、全网状连接和部分网状连接。

(1) 星状连接(Hub&Spoke)。适用于公司分部与总部业务占所有业务流量的大多数，而公司分部与公司分部之间业务流量很少的情况。这样，所有分部业务都与总部建立有直连的 IP 虚连接(或者与最近的结点具有直连连接，形成分级式的组网)，分部和分部之间的业务流量经过总部(或上级结点)转发来完成，这样整个组网的成本最低，而且方便进行访问控制，如图 7-3 所示。

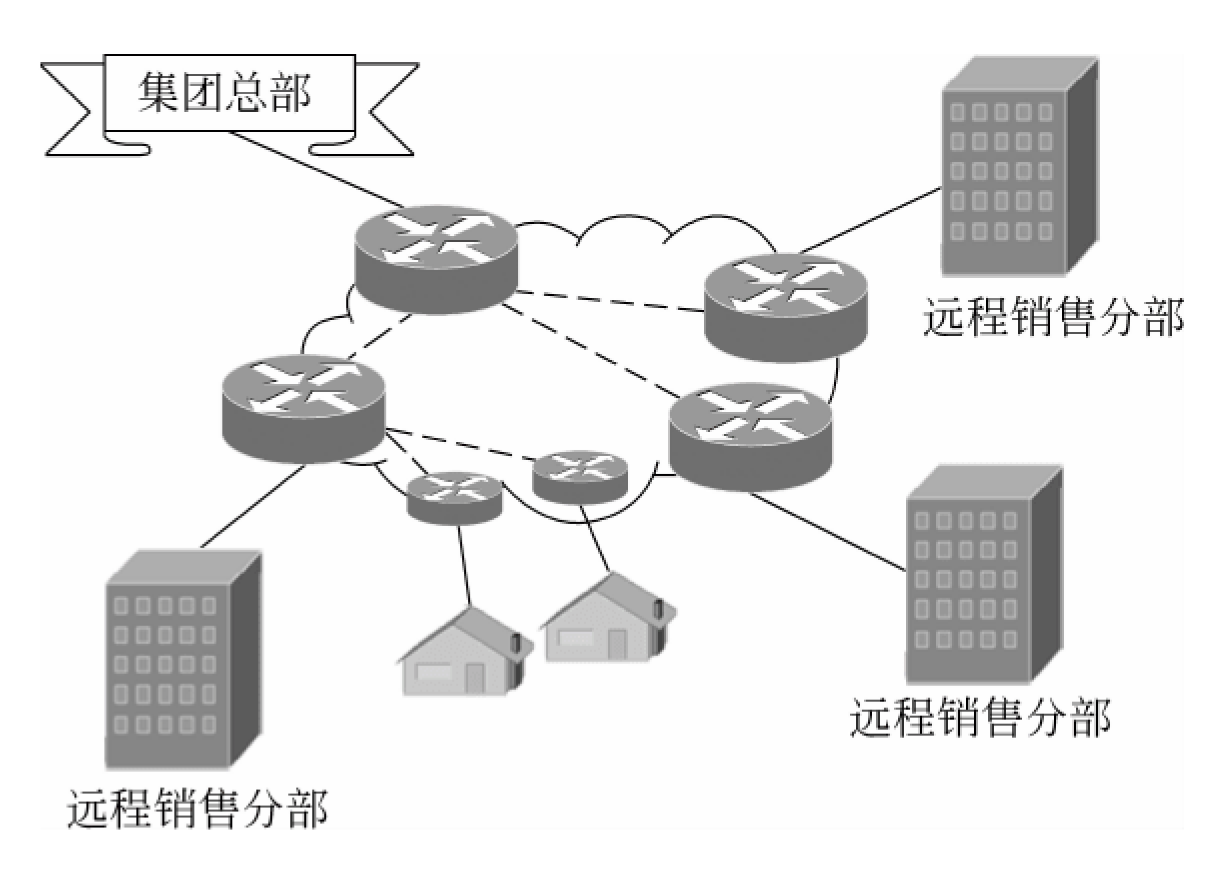


图 7-3　星状连接的内联网 VPN

(2) 全网状连接(Full Mesh)。适合做各个公司分部与公司总部之间业务量比较均衡的情况，在所有站点之间建立直连的 IP 虚连接，这样整个组网的成本最高，但站点间业务访问的效率也最高，如图 7-4 所示。

(3) 部分网状连接(Partial Mesh)。部分站点间有较大业务流量需求，又有部分站点只有很少业务流量需求，这样可以采用综合上面两种方式的部分网状连接模式，成本居中，效率也可以满足企业客户的需要，如图 7-5 所示。

图 7-4　全网状连接的内联网 VPN

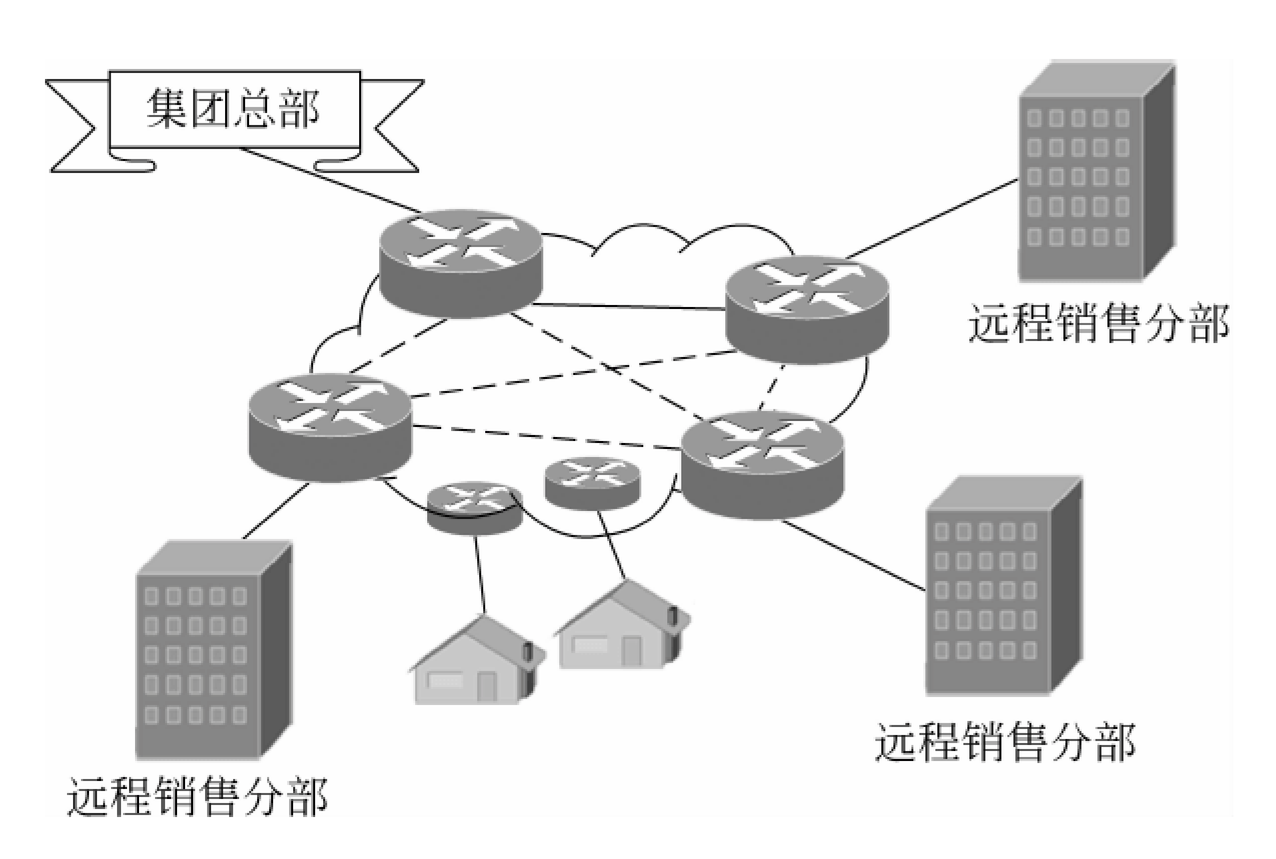


图 7-5　部分网状连接的内联网 VPN

7.5.2　企业外部虚拟网

企业外部网的 VPN 建立在集团与其用户或供应商之间，或者企业间发生收购、兼并或企业间建立战略联盟后，使不同企业网通过公网来构筑的虚拟网。如图 7-6 所示，企业外部网允许通过目前用于 Web 浏览器的 HTTP 协议来访问，或使用别的经相关部门认可的服务和协议来建立连接。企业外部网的 VPN 包括必需的接入控制以及鉴别机制，

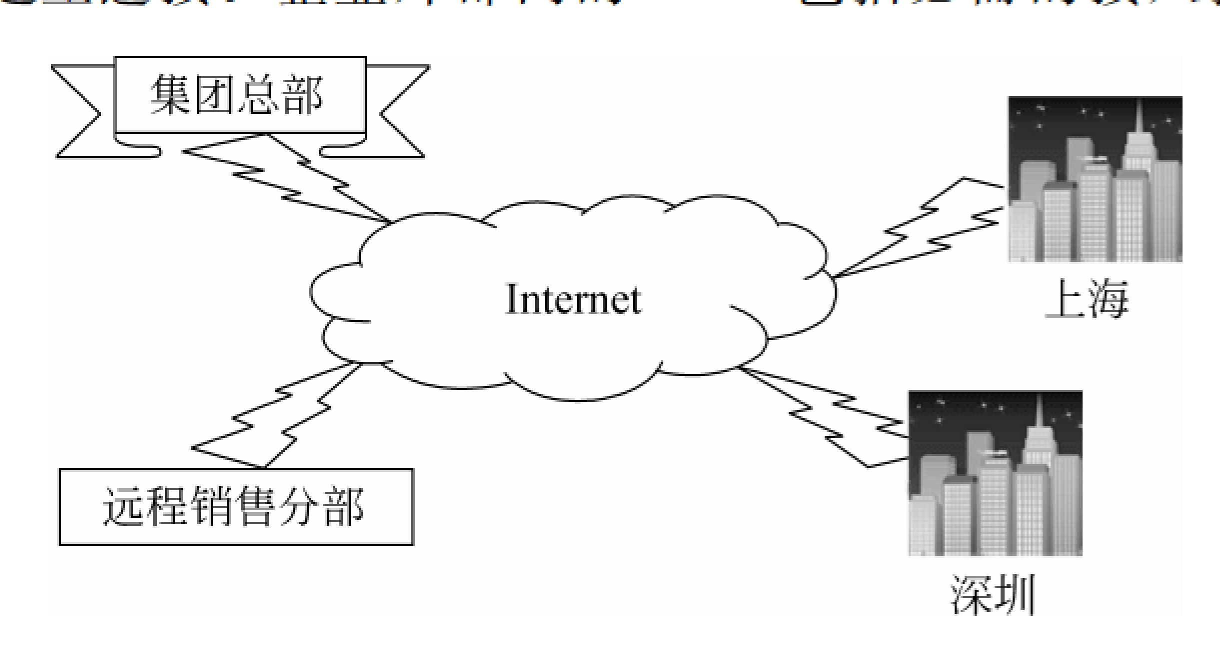


图 7-6　企业外部互联的 VPN

使包括合作企业和客户在内的不同用户群能够访问企业的服务和数据。通过制订不同的策略可以实现这一目的，具体可通过防火墙、带访问列表功能的路由器、应用网关或者能够采用传输流量策略的其他设备来实现。这种方式使集团能够安全有效地与其主要贸易伙伴和客户相处，主要优势在于速度以及业务效率的提高，这就是电子商务最具影响力之处。

企业外部虚拟网(Extranet VPN)与 Intranet VPN 没有本质区别，但它涉及的是不同公司网络间的通信，所以它要更多地考虑设备的互连、地址的协调、安全策略的协商等问题。

(1) 地址协调。目前，由于 IP 地址资源紧张，所有企业网的地址规划一般都采用私网地址空间，也就是说，企业与企业之间的 IP 地址很可能重叠。在 IP 网络中，IP 地址是一台主机的唯一标识，不允许重叠，而外联网 VPN 又将不同企业的子网连接到一起，这就会不可避免地出现地址协调的问题。主要有如下两种方式。

① 所有互联部分需要统一规划地址，这样就可以防止由于地址空间重叠造成无法实现互通的问题。

② 采用地址转换技术(NAT)，不仅仅按照源/目的地址进行转换，甚至还可能需要按照用户标识、接入等策略实现转换。对于 VPN 业务，NAT 技术还没有完整的标准，但基本可以解决互联的地址重叠问题。

(2) 验证/授权机制。根据不同的接入方式选择不同的认证方式，比如采用 PPPoE (PPP over Ethernet)接入，可以支持利用 RADIUS 服务器完成 PAP/CHAP 验证等，采用 Portal 模式接入的用户可以采用 Web 验证方式。

(3) 信息扩散范围的限制。消息传递在各个用户之间是受限的，比如，即便采用了加密方式确保安全，企业与银行的结算信息也不应该扩散到其他客户中。这可以采用路由策略发布、广播域隔离、防火墙等方案。

7.5.3 远程接入虚拟网

远程接入虚拟网(Access VPN)建立于集团总部与远程移动用户之间，最适用于公司内部经常有流动人员远程办公的情况。图 7-7 描述了到 VPN 的最常用的连接方式，通过在远端电脑上加载加密软件，个人也可以建立一个通向集团总部 VPN 设备的加密隧道。

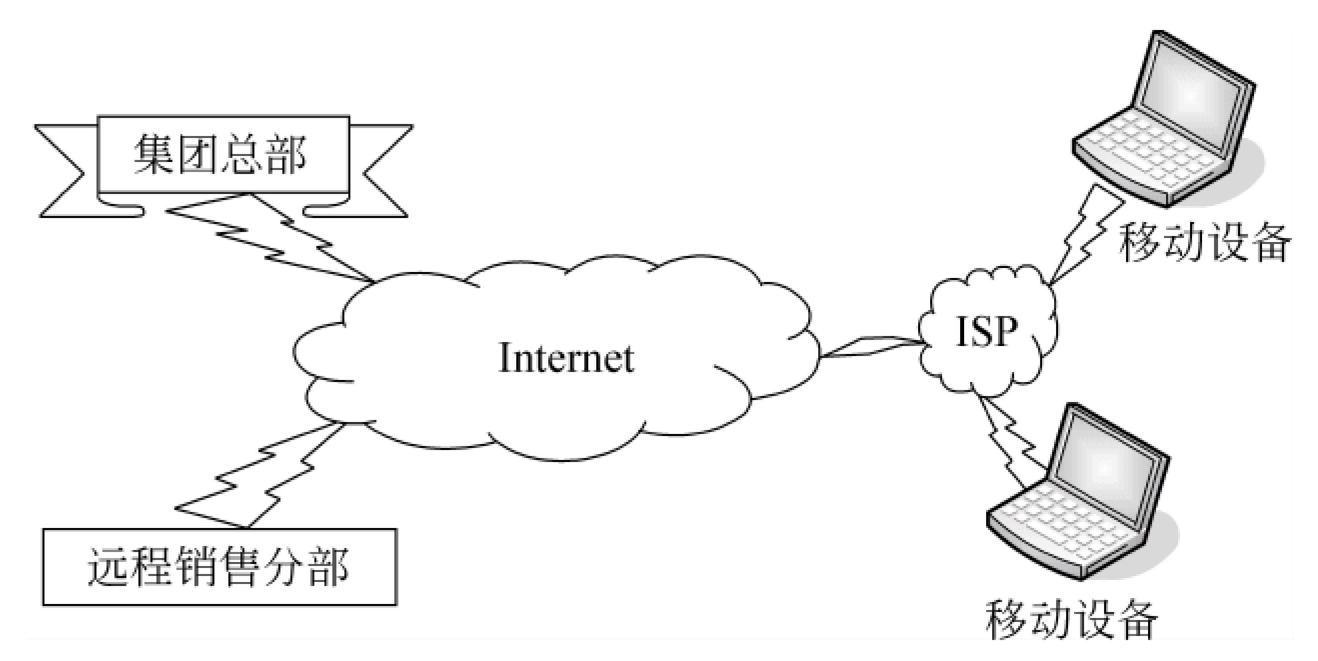


图 7-7 远程接入 VPN

远程接入支持远程用户采用PSTN、ISDN、DSL、电缆(Cable Modem)或无线的方式接入企业网络。基于VPN的远程接入业务能够为企业提供一种更为经济有效的接入解决方案,满足他们移动和远程办公应用的需求,包括电子邮件、文件共享及数据库访问等。采用远程接入VPN,企业不再需要配置和维护远程接入交换机(RAS)、宽带RAS,或者由这些设备到总部站点之间的专用链路,大大降低了运营和管理成本。

7.6 VPN的体系结构

不同的网络基础结构以及公司的不同需求要求有不同类型的VPN体系结构。VPN的体系结构包括独立于操作系统的黑匣VPN、基于路由器的VPN、基于防火墙的VPN和基于软件的VPN等。除了这些结构,还可以在不同种类的VPN设备上添加其他服务和特性,比如用户认证、Web过滤器和防病毒软件。然而,添加这些服务和特性时,要在产品的有效服务数量、运行这些服务所需的处理需求以及这些服务的最终支持之间做一个权衡。下面将分别介绍不同类型的VPN体系结构。

7.6.1 网络服务供应商提供的VPN

这是使公司与Internet联网并享受VPN提供服务的最简单有效的方法。网络服务供应商将在公司现场放置一个设备,来创建VPN隧道,然而这不是唯一的方案。一些ISP可以安装一个前端PPTP交换机,它可以自动创建VPN隧道。通信的目的端将对信息分组进行解密,并把数据发送到主机。

防火墙也可能被添加到这种类型的环境中,通常在网络设备前端或其中间。与以往建立DMZ(Demilitarized Zone)的方法类似,内部路由器连接到防火墙的一个端口上,防火墙的另一个端口连接到外部的路由器上,外部路由器的串行口连接到ISP上。用户要注意IP地址、路由以及邮件之类的问题。图7-8描述了一个典型的网络设备供应商的VPN解决方案。

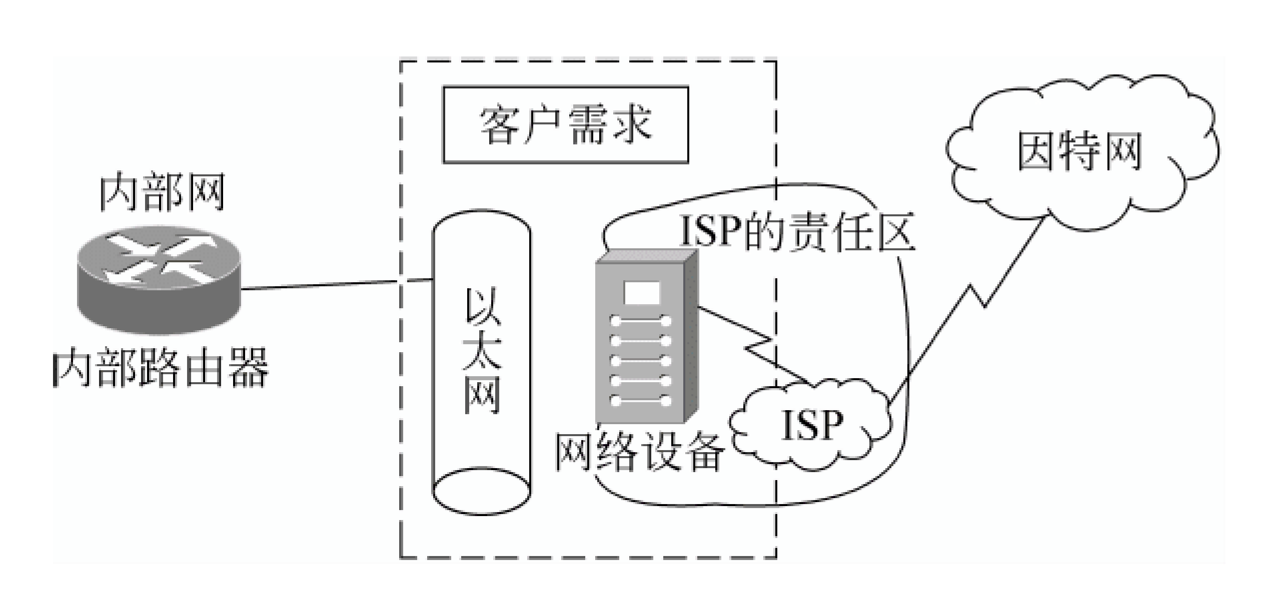


图7-8 网络服务器提供的VPN

ISP在网上安装一台设备或者安装一台可以自动创建VPN隧道的前端VPN交换机。服务供应商负责与这台设备通信有关的设备,图7-8中清楚地定义了责任范围。

7.6.2 基于防火墙的 VPN

基于防火墙的 VPN 是 VPN 最常见的一种实现方式，许多厂商都提供这种配置类型。因为绝大部分公司都会使用防火墙连向 Internet，实现 VPN 所需要的只是增加加密软件，而且现在购买防火墙时，都会带有实现 VPN 加密技术的能力。

基于防火墙的 VPN 充分利用防火墙的安全机制，包括对内部网络的访问限制。它还执行地址转换，符合强认证要求，发出实时警报，并提供广泛记录功能。当远程用户或网络有可能不友善时，最好选择基于防火墙的 VPN。网络管理员建立一个所谓的停火区(DMZ)网段，一般在防火墙使用一个第三方接口，配以之间的访问控制规则。黑客可能会进入停火区，但他们不能破坏内部网段。对于纯内部网来说，使用基于防火墙的 VPN 很经济，而且易于加固和管理。

考虑基于防火墙的 VPN 时，有很多厂商可供选择，其产品在所有不同的平台上都能有效使用。一个非常重要的安全性考虑是关于下层操作系统的。防火墙在什么平台上运行？是基于 UNIX，基于 Windows NT，还是别的平台？该操作系统潜在的缺陷是什么？没有百分之百安全的设备。因此，如果在防火墙设备上建立 VPN，需要确认底层的操作系统是安全的。此外，大多数商用防火墙会把主机操作系统的冒险服务或多余服务关闭，从而加固操作系统内核。操作系统保护是一种主要的附加功能，没有几家 VPN 供应商提供有关操作系统安全性的指导。图 7-9 为基于防火墙的 VPN。

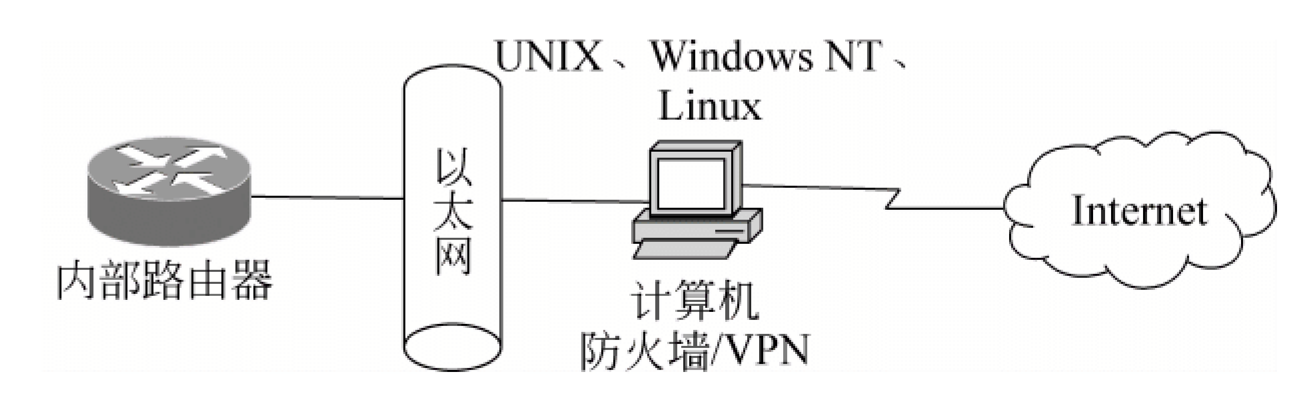


图 7-9 基于防火墙的 VPN

7.6.3 基于黑匣的 VPN

在黑匣方式中，厂商只提供一个黑匣，这是加载了加密软件，以创建 VPN 隧道的一个基本设备。一些黑匣附带有运行于台式客户机上帮助进行设备管理的软件，而另一些可以通过 Web 浏览器进行配置。这些硬件的加密设备比软件类型的加密设备速度更快，它们可以建立所需的加速隧道，更快地执行加密进程。并非所有的黑匣子都提供集中管理功能，它们通常并不支持自身记录，而需要把这些记录发送到另一个数据库查询。如果要进行认证，还需要一个服务器。

目前，厂商应该支持所有的 3 种隧道协议：PPTP、L2TP 和 IPSec，但也不是必需的。大多数黑匣设备都需要一个独立的防火墙，所以更多的厂商正准备把基于黑匣的 VPN 与防火墙功能合并起来。图 7-10 为基于黑匣的 VPN。

基于黑匣的 VPN 设备可以装在防火墙之后，也可以装在防火墙旁边，如图 7-11 所

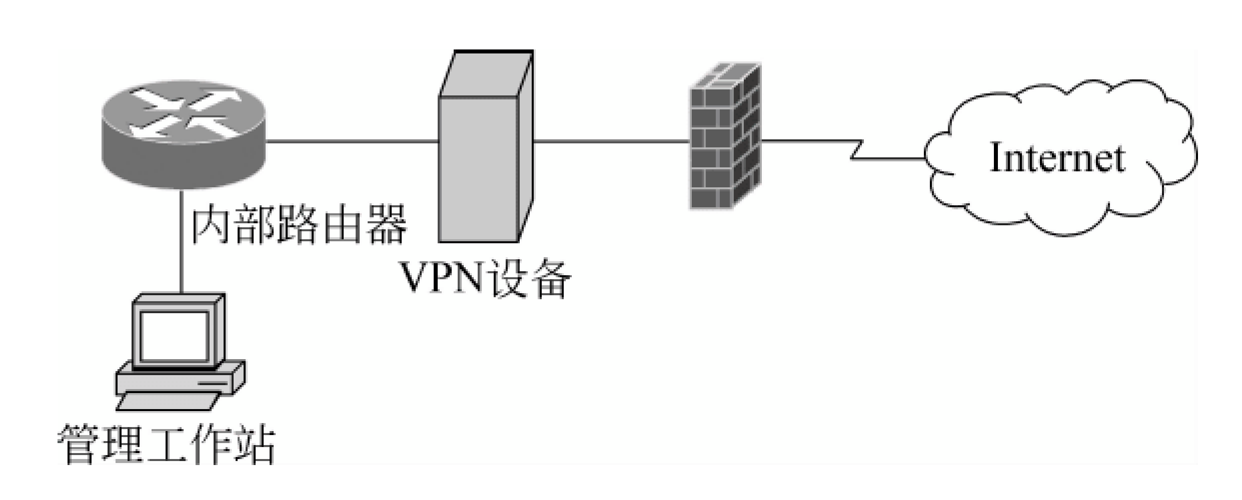


图 7-10 基于黑匣的 VPN

示。防火墙向公司提供安全保证,但它并不保证数据安全。同样,VPN 设备保证数据的安全,但并不向公司提供安全保证。一些黑匣子通过命令行语法进行配置,但是大多数都拥有基于 Web 的 GUI。

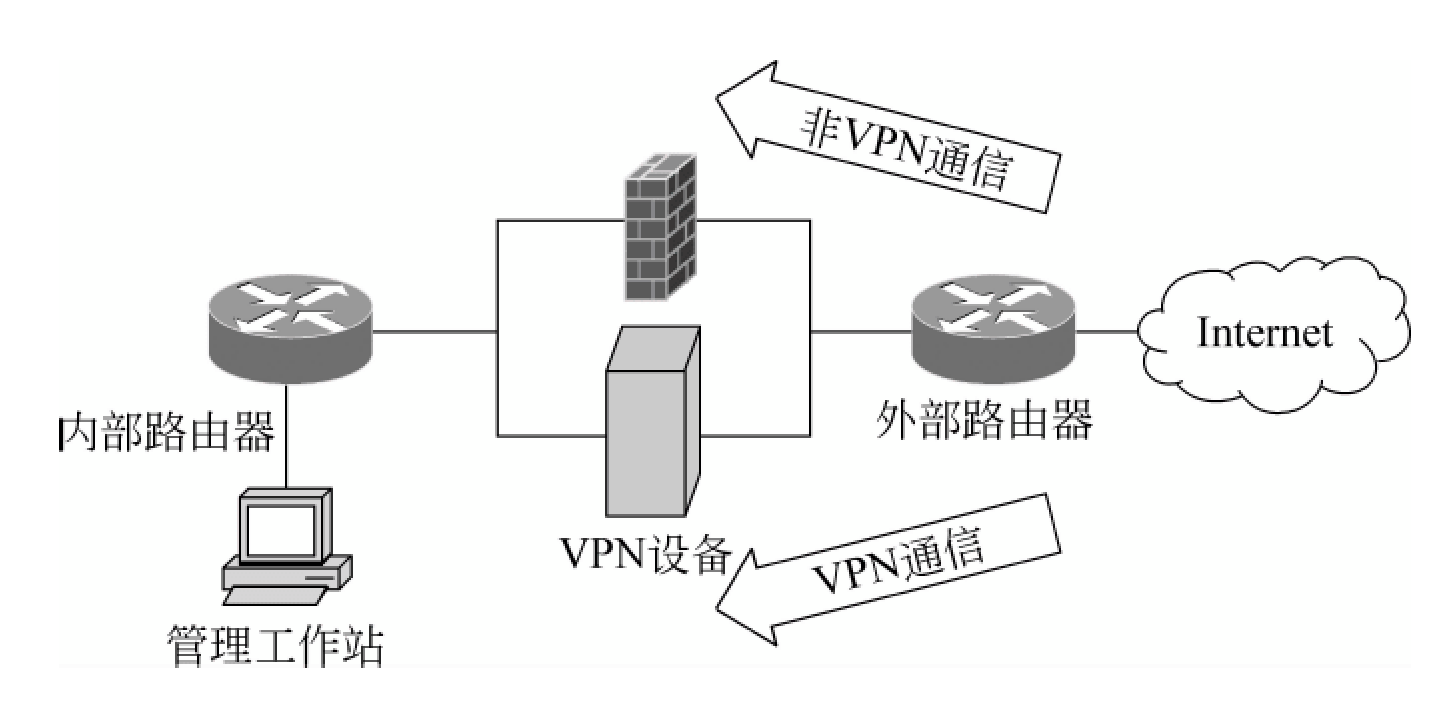


图 7-11 与防火墙并列的 VPN

需要注意的是,防火墙上可能安装了一个基于规则的策略。对于防火墙在 VPN 设备前面的情况,在防火墙的配置中,要保证能传递 VPN 加密的分组。防火墙是起保护作用的,如果在 TCP 端口上进行过滤,而进来的分组是加密的,防火墙就会检查这些分组,发现是"陌生的"就会丢弃。因此,必须确定防火墙能使这些分组通过。

7.6.4 基于路由器的 VPN

基于路由器的 VPN 适用于有实力投巨资购买路由器的公司,且公司中具备这方面经验的员工。许多经营路由器的厂商支持这种配置,访问其网页可以得到相关的配置示例。VPN 路由器的服务功能包括带宽管理、QoS、网络拥塞控制、流量、整形以及对常用路由协议的功能增强。

基于路由器的 VPN 有两种,一种方法是把软件加载到路由器上,以进行加密处理;另一种方法把另一个厂商的卡插入与路由器一起的机架中。第二种方法把加密处理从路由器的 CPU 转移到附加的卡上。

一些厂商支持热备份以及冗余,这些被设置在其基于路由器的 VPN 产品中,对那些只允许很短停机时间的公司来说非常必要。对于基于路由器的 VPN 来说,性能是一个重要的问题。由于在路由程序中增加加密程序,给路由器加重了负担,尤其当路由器正在处理大量的路由问题时,或者正在实现增强的路由算法的时候,更是如此。图 7-12 是一

个典型的基于路由器的 VPN，其中分组从源端到目的端（如总部到远程的分部）都被加密。

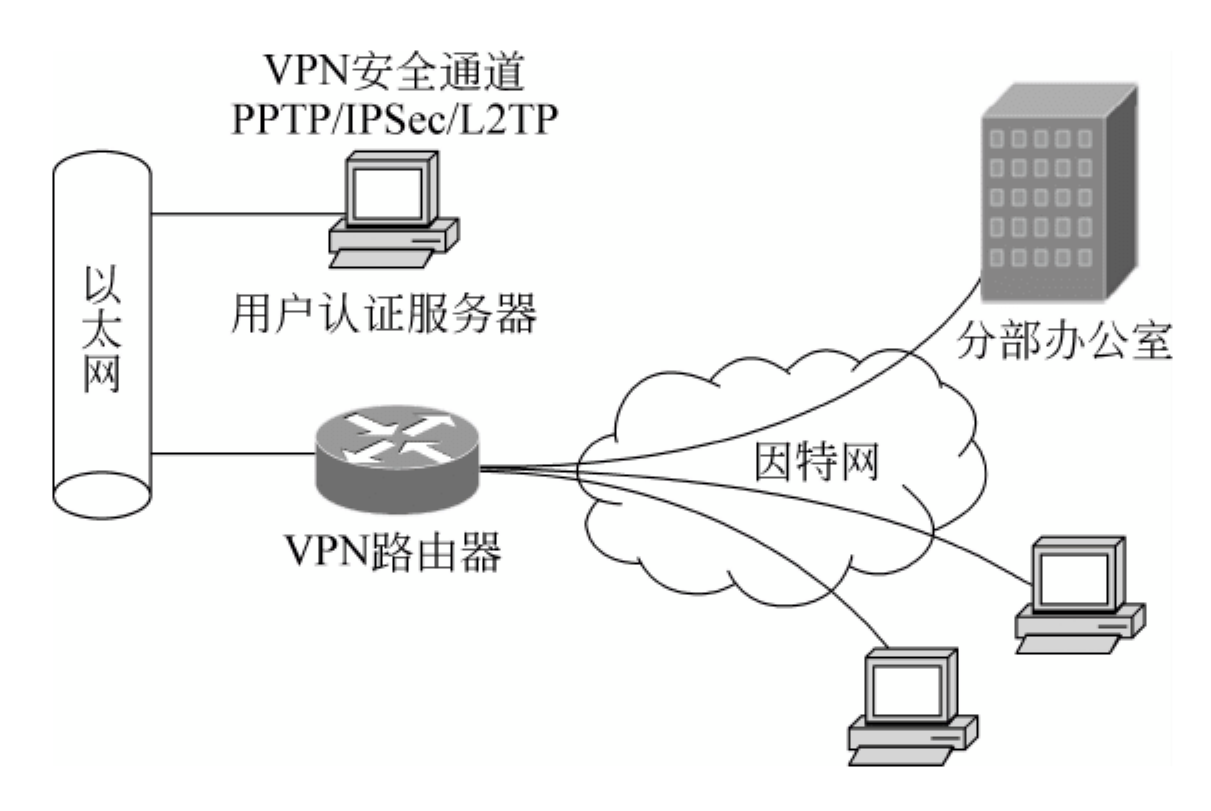


图 7-12　基于路由器的 VPN

7.6.5　基于软件的 VPN

基于软件的 VPN 基本上是建立到另一主机的隧道或予以加密的软件，它通常用于客户机到服务器之间。举例来说，这个 PPTP 的 VPN 中，客户机上加载的软件连接到在服务器上加载的软件，并且建立一个 VPN 会话。还有别的类型的软件 VPN。当选择软件 VPN 的时候，需要有一个很好的密钥管理程序，还需要一个证书管理机构。对于别的类型的 VPN（如防火墙/VPN 到防火墙/VPN）来说，唯一需要的密钥是从 VPN 到 VPN 的。也就是说，内部网上的通信量是解密过的，因此，只需要 VPN 设备的密钥。但是，在客户机到服务器的情况下，每个位置都可能有一对专用/公共的密钥。图 7-13 为基于软件的 VPN。

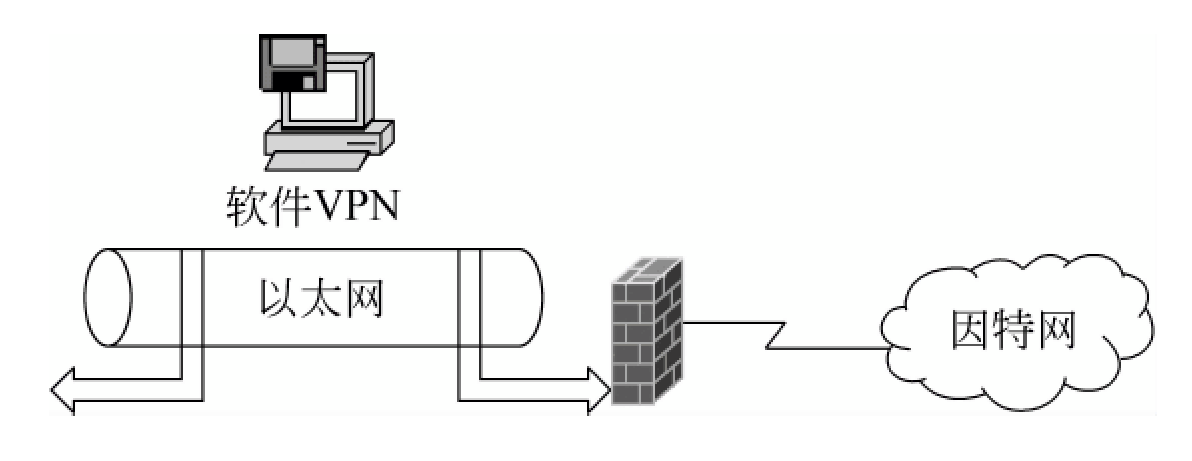


图 7-13　基于软件的 VPN

软件 VPN 一般都采用 Windows 操作系统，硬件 VPN 一般采用专用操作系统来实现的。基于硬件的 VPN 产品的安全性比软件产品好，如果连接速度在 T1（1.544Mbps）以上，应该首选硬件产品。基于软件的 VPN 可能更为灵活，硬件产品一般不是根据协议给所有通信量建立相应的隧道，而软件产品根据地址或协议建立隧道。如果远程站的混合通信量的一部分通过 VPN 传输，而另一部分不通过 VPN 传输，根据通信量类型建立隧道有好处。在性能要求适中的情况下（例如用户采用拨号连接），软件产品可能是最好的选择。另外，使用硬件产品在每个端点站必须使用定制硬件，每次更改网络拓扑或者取

消用户密钥时，某些早期产品要求人工更改每个端点站。

基于软件的问题通常是难以管理。这要求管理员熟悉主机操作系统、应用程序以及适当的安全机制。某些软件包要求对路由选择表和网络寻址模式作某些更改。

综上所述，如果客户对一般软件使用和 Windows 系统十分熟悉，建设的网络结构比较简单，对网络性能、QoS 无十分严格的要求，正好又有闲置的、高配置的、装有正版 Windows 系统的计算机，软件产品可以在一定程度上体现价格优势。

如果建立的 VPN 网络考虑系统安全、长期稳定运行、维护成本、良好的综合性能等因素，硬件 VPN 产品具有软件产品不可比拟的优势。

7.6.6 性能比较

每种 VPN 体系结构都有自己的优点和缺点，如表 7-1 所示。在选择时，要考虑很多不同的因素，比如安全性、用户认证和访问、内部网络基础结构的互操作性以及外部客户和供应商的互操作性等。

表 7-1 VPN 体系结构性能比较

VPN 体系结构	优　点	缺　点
硬件	性能好；安全性好；较大的分组加密开销最小；一些支持负载平衡	灵活性有限；开销大；没有 ATM、FDDI 或令牌环接口；大部分是半双工的；改变设置后需要重启；一些对小的分组（64 位）来说有性能问题；子网功能有限；有些产品缺乏 NAT
软件	支持的平台范围广；安装简易；适用范围广	NAT 支持性能问题；一些还使用旧的加密技术；一些缺乏远程管理能力；没有监控能力
路由器	利用现有硬件；强大有效的安全性；使用已有路由器，因而开销较小	一些可能需要额外的加密卡；存在性能问题；需要升级成为更强大的路由器
防火墙	支持的平台范围广；利用已经存在的硬件；一些支持负载平衡以及冗余的防火墙；IPSec 开销小	操作系统可能带来安全问题；RADIUS 并不能支持完整的互操作性；某些涉及使用许可问题

7.7 VPN 设备

在描述各种 VPN 技术之前，需要先介绍一下 VPN 设备。根据在网络上的位置，VPN 设备可以分为服务运营商设备和用户设备，如图 7-14 所示。

其中客户端设备分为两类，内容如下。

（1）用户设备（Customer Devices）。用户设备是位于用户网络中的简单设备，可以是路由器或者交换机。这些设备不直接连接到服务运营商的网络。

（2）用户边缘（Customer Edge，CE）设备。位于用户网络的边缘，和服务运营商网络相连，为用户提供对服务运营商的接入。CE 设备可以是一台交换机或是一台 IP 路由器，

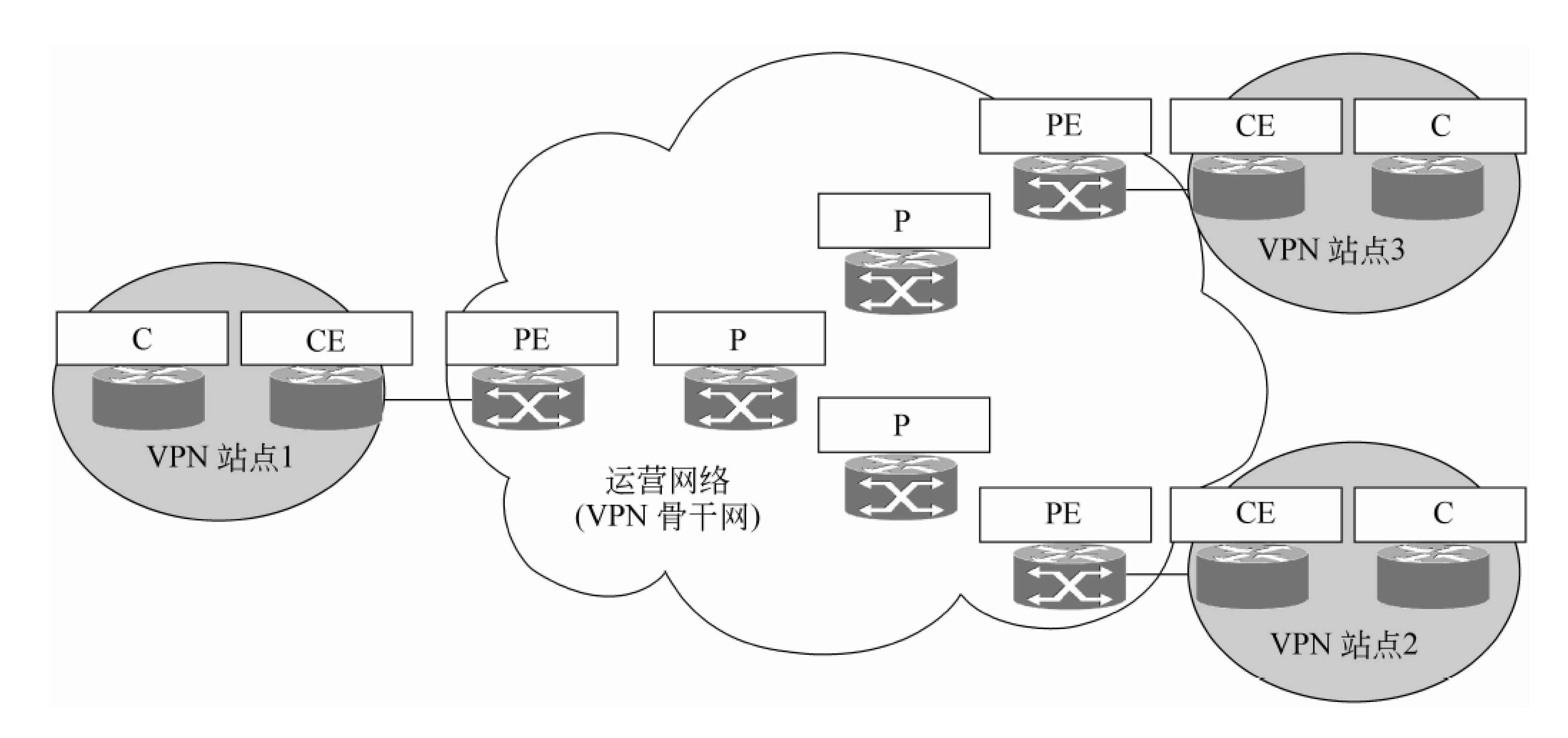


图 7-14　VPN 设备

它与直连的 PE 路由器建立邻接关系。建立邻接关系后，CE 路由器将站点的本地路由广播给 PE 路由器，并从该 PE 路由器学习到远端 VPN 路由。

在站点到站点 VPN 中，服务提供商网络设备也分为两类，内容如下。

（1）服务运营商(Provider，P)设备。是位于服务运营商网络中的设备，可以是路由器或者交换机。这些设备不直接连接到用户网络中。

（2）服务运营商边缘(Provider Edge，PE)设备。服务运营商边缘设备直接和用户网络相连。

基于 CE 的 VPN，又称为基于客户的 VPN，是指 VPN 信息只是在客户网络的边缘设备(CE)中，如图 7-15 所示。这时，所有与 VPN 相关的特定处理都是在 CE 设备中完成的，VPN 业务的起始点和终止点都是面向客户网络的，其内部技术构成、拓扑、编址、实施和管理都对 VPN 客户网络可见。运营商网络并不知道客户网络的路由或编址的任何信息，感知不到客户 VPN 的存在，提供的只是简单的 IP 服务，只为具有全球唯一地址的 IP 分组提供服务。

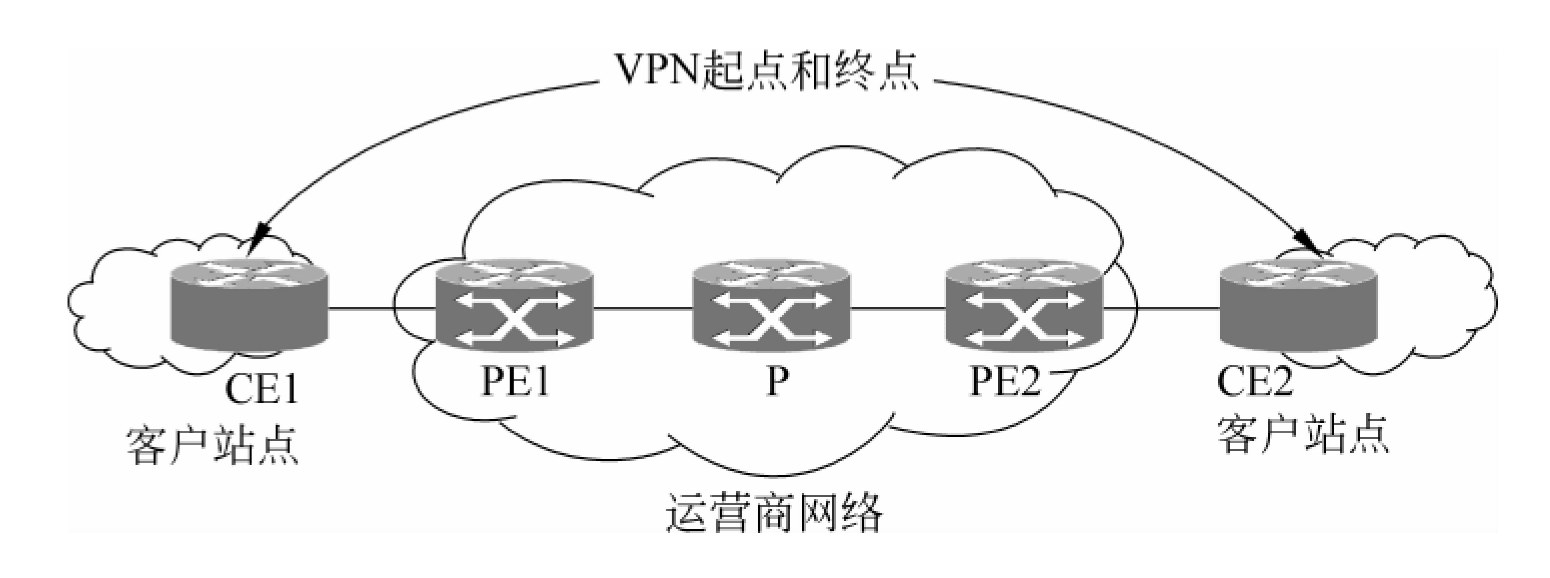


图 7-15　基于 CE 的 VPN

对于基于 CE 的 VPN，其实施和管理可以由用户自己做，也可以委托给运营商来实施和管理(即所谓的运营商实施的基于 CE 的 VPN)。在运营商实施的基于 CE 的 VPN 中，VPN 业务是一种由受信的第三方(运营商)负责部署企业所希望的 VPN，并代表企业进行实施和管理，所使用的 VPN 相关特定设备位于运营商网络和客户网络的边界用户

一侧。委托管理可以降低对客户的技术要求,也可以降低业务的建设和运营成本。

基于PE的VPN(又称为基于网络的VPN),是指VPN信息只是在运营商网络的边缘设备(PE)中,如图7-16所示。在基于PE的VPN中,所有与VPN相关的特定处理都是在PE设备中完成的,客户并不知道VPN的任何信息,CE设备感知不到是否有VPN的存在。

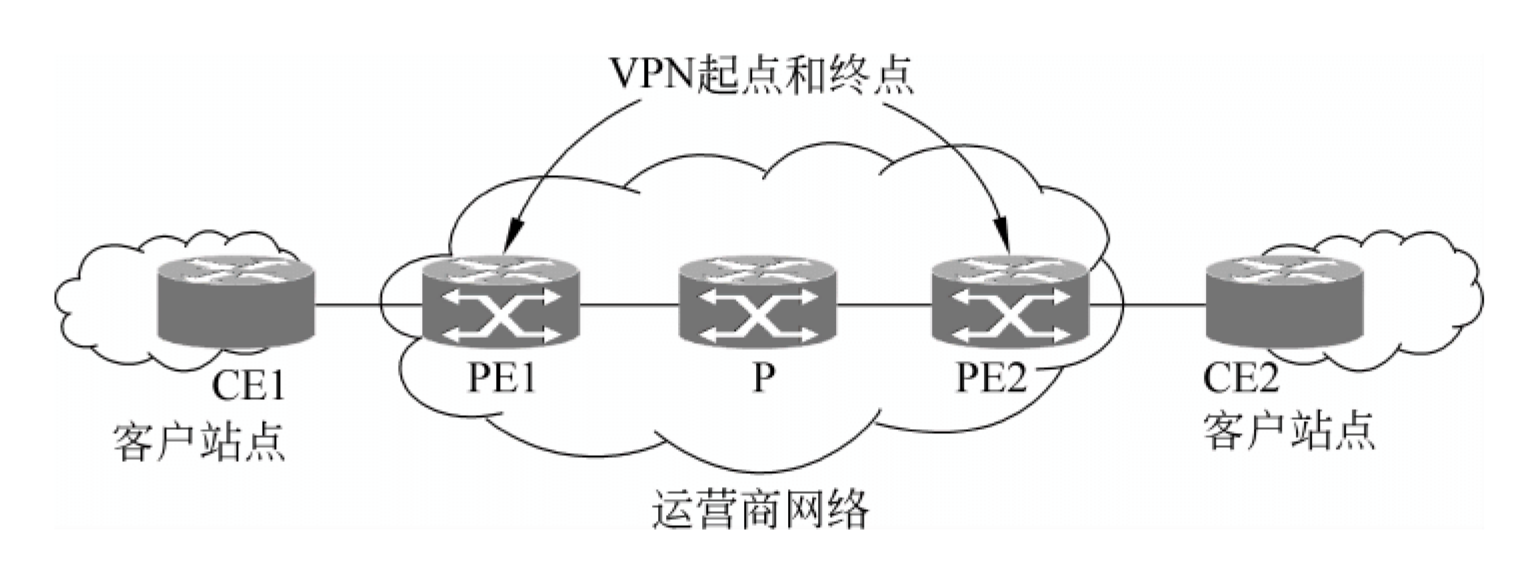


图7-16 基于PE的VPN

基于PE的VPN,通常也叫做服务器发起的VPN或强制方式的VPN。在这种方式的VPN中,VPN的整个操作作为一个ISP的外包资源,实现在运营商网络的边缘设备上,而不是用户CE上,这样在简化用户复杂度、增加业务灵活性和扩展性的同时,也为运营商带来了新的收入。根据客户和运营商之间交互可达性信息的协议层次,一般可以把基于PE的VPN进一步划分为三层VPN和二层VPN两类。

在基于PE的VPN中,PE设备属于运营商所有,因此一般都是运营商负责实施和管理的。当然,也允许用户在一定程度上进行VPN业务的管理和控制。

7.8 VPN网络使用的安全技术

VPN传输的是私有信息,因此VPN用户对数据的安全性非常重视。目前,VPN主要采用4项技术来保证安全,分别是隧道技术(Tunneling)、加解密技术(Encryption & Decryption)、密钥管理技术(Key Management)、使用者与设备身份认证技术(Authentication)。

7.8.1 隧道技术

VPN的核心是"隧道"技术。隧道技术通过对数据进行封装,在公共网络上建立一条数据通道(隧道),让数据包通过这条隧道传输。隧道技术是一种通过使用互联网络的基础设施,在网络之间传递数据的方式,使用隧道传递的数据(或负载),可以是不同协议的数据帧或包。隧道协议将这些其他协议的数据帧或包重新封装在新的包头中发送,这个过程称作挖隧道。新的包头提供了路由信息,从而使封装的负载数据能够通过互连网络传递。

隧道是由隧道协议形成的。为了能够在VPN上传递数据包,并提供一定的安全性和服务质量保证,VPN必须采用一种或多种隧道协议。一个隧道协议通常包括以下3个

方面的内容。

(1) 乘客协议。被封装的协议,如 PPP、SLIP 等。

(2) 封装协议。隧道的建立、维持和断开,如 L2TP、IPSec 等。

(3) 承载协议。承载经过封装后的数据包的协议,如 IP 和 ATM 等。

隧道协议可以工作在协议栈的不同层次,表 7-2 是 TCP/IP 协议栈中典型隧道协议的工作层次。需要注意的是,某些隧道协议不只是一个协议,而是一个协议族,这种隧道协议族往往可能工作在协议栈的多个层次。如 IPSec 协议族,它的认证头(AH)协议和封装安全载荷(ESP)协议工作在网络层,而 Internet 密钥交换协议(IKE)却工作在应用层(基于 UDP)。

表 7-2 典型隧道协议的工作层次

OSI 七层模型	安全技术	典型隧道协议
应用层	应用代理	S-MIME/IKE
表示层		
会话层	会话代理	SOCKSv5/SSL/TLS
传输层		
网络层	包过滤	IPSec (AH,ESP)/IP-in-IP/GRE
数据链路层		L2TP/PPTP/L2F/MPLS
物理层		

隧道协议可以分为 3 类:第二层隧道协议、第三层隧道协议和高层隧道协议。不同层次的区别主要在于用户数据中网络协议栈的第几层被封装。

1. 第二层隧道协议

第二层隧道协议是在数据链路层进行的。先把各种网络协议封装到 PPP 包中,再把整个数据包装入隧道协议中,这种经过两层封装的数据包由第二层协议进行传输。

第二层隧道协议有以下 4 种。

(1) PPTP(RFC 2637,Point-to-Point Tunneling Protocol)。

(2) L2F(RFC 2341,Layer 2 Forwarding)。

(3) L2TP(RFC 2661,Layer Two Tunneling Protocol)。

(4) MPLS(RFC 3031,Muti-Protocol Label Switch)。

PPTP、L2F、L2TP 协议详见第 2 章,本节将介绍多协议标记交换(MPLS)。

RFC3031 定义的多协议标记交换(Multi-Protocol Label Switch,MPLS)是一种二层交换和三层路由结合起来的技术。设计 MPLS 的主要目的是对标记交换转发与网络路由的集成技术进行标准化。使用标记交换能够提高网络层路由的性能/价格比,改善网络层的可扩展性,并为路由服务提供更好的灵活性。MPLS 的早期工作集中在 IPv4 上,其核心技术可扩展到多种网络协议上,包括 IPv6、IPX、AppleTalk、DECnet 以及 CLNP 等。此外,MPLS 也不局限于特定的链路层技术,它能在网络层实体间使用多种链路层介质传

输网络层分组，如 Ethernet、PPP、ATM 以及 FR 等。MPLS 与上下层协议的关系如图 7-17 所示。

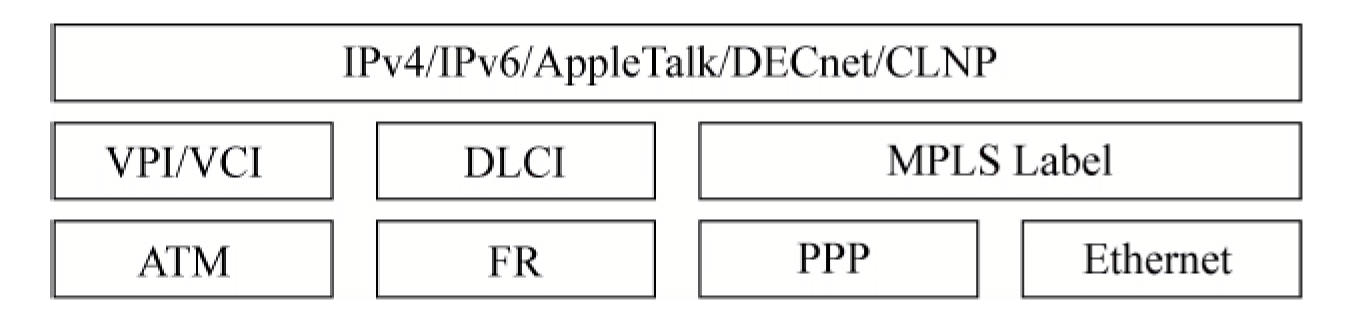


图 7-17　MPLS 的多协议支持

MPLS 允许作为不同链路层技术的交换技术像同层 VPN 技术一样运行，并处于第二层的传输和交换环境中。因此，将 MPLS 看做第二层 VPN 隧道技术。MPLS 的主要观点就是为每个包分配一个固定长度的短标签，交换机根据这些简单标签来决定数据如何进行转发。与此形成鲜明对比的是传统的第三层路由，传统的第三层 IP 路由包含对每个包非常复杂的转发分析，每个路由器都对第三层包头中的转发信息进行处理，然后根据路由表来决定下一步的转发目的。

在 MPLS 中，只对第三层的信息进行一次详细的分析。这个工作在网络边缘的标签交换路由器(LSR)上进行，只有那些具有固定长度标签的数据包被发送。在网络的另一端，客户的边缘路由器从数据包头中取出正确的标签信息。转化决定可以在对固定长度标签的一次查询中得到，这就是 MPLS 最关键的性能增强。

MPLS VPN 不依靠封装和加密技术，而是依靠转发表和数据包的标签来创建一个安全的 VPN。每个 VPN 对应一个 VPN 路由/转发实例(VRF)。一个 VRF 定义了同 PE 路由器相连的客户站点的 VPN 成员资格。一个 VRF 数据包括一个 IP 路由表、一个派生的 CEF(Cisco Express Forwarding)表、一套使用转发表的接口、一套控制路由表中信息的规则和路由协议参数。一个站点可以且仅能同一个 VRF 相联系，客户站点 VRF 中的数据包含其所在的 VPN 中所有可能连到该站点的路由。在 VRF 中定义的和 VPN 业务有关的两个重要参数是 RD(Route Distinguished，路由分布)和 RT(Route Target)。RD 和 RT 的长度都是 64 位。

对于每个 VRF，数据包转发信息存储在 IP 路由表和 CEF 表中，每个 VRF 维护一个单独的路由表和 CEF 表。这些表可以防止转发信息被传输到 VPN 之外，同时也能阻止 VPN 之外的数据包转发到 VPN 内部的路由器中。这个机制使得 VPN 具有安全性。

在每个 VPN 内部，用户可以建立任何连接：每个站点可以直接发送 IP 数据包到 VPN 中的另一个站点，无须穿越中心站点。一个路由识别器(RD)可以识别每一个单独的 VPN，一个 MPLS 网络可以支持成千上万个 VPN。每个 MPLS VPN 网络的内部是由供应商(P)设备组成的，这些设备构成了 MPLS 核心，且不直接同 CE 路由器相连。围绕在 P 设备周围的供应商边缘路由器(PE)可以让 MPLS VPN 网络发挥 VPN 的作用。P 和 PE 路由器称为标签交换路由器(LSR)，LSR 设备基于标签来交换数据包。客户站点可以通过不同的方式连接到 PE 路由器，例如帧中继、ATM、DSL 和 T1 方式等。

在 MPLS VPN 中，用户站点通常运行的是 IP，它们并不需要运行 MPLS、IPSec 或者

其他特殊的VPN协议。在PE路由器中,RD对应同每个用户站点的连接,这些连接可以是诸如T1、单一的帧中继、ATM虚电路或者DSL等物理连接。RD在PE路由器中被配置,是设置VPN站点工作的一部分,它并不在用户设备上配置,对于用户来说是透明的。

每个MPLS VPN具有自己的路由表,这样用户可以重叠使用地址,且互不影响。例如,任何数量的用户都可以在MPLS VPN中使用地址为10.1.1.X的网络。MPLS VPN的一个最大的优点是CPE设备不需要智能化,因为所有的VPN功能是在互联网络的核心网络中实现的,且对CPE是透明的,CPE并不需要理解VPN,同时也不需要支持IPSec。这意味着用户可以使用价格便宜的CPE,甚至可以继续使用已有的CPE。

因为数据包不再经过封装或者加密,所以时延被降到最低。之所以不再需要加密,是因为MPLS VPN可以创建一个专用网,它同帧中继网络具备的安全性很相似。因为不需要隧道,所以要创建一个全网状的VPN网也将变得很容易。事实上,默认的配置是全网状布局,站点直接连到PE,之后可以到达VPN中的任何其他站点。如果不能连通到中心站点,远程站点之间仍然能够相互通信。

MPLS可以提供很好的VPN性能,它的LSP可以隔离从不同地点流出的数据,从而保证数据流的私密性。另外,MPLS综合了BGP协议,分发BGP在对等体间的可达性信息,并且允许每个BGP结点通过学习,了解相同VPN里直接连接于用户端的对等体的信息。由于BGP对等体为每个VPN端点交换标签,每个BGP端点可以自动建立MPLS隧道(LSP),包含相同VPN里直接隶属于用户端对等体的VPN专用LSP。因此,MPLS可以在一个共享的IP网络中自动提供一个完全网状的VPN连接,当结合MPLS的流量工程特性后,MPLS VPN也可为用户提供不同等级的服务。

2. 第三层隧道协议

第三层隧道协议是在网络层进行的,把各种网络协议直接装入隧道协议中,形成的数据包依靠第三层协议传输。第三层隧道协议有以下3种,内容如下。

(1) IP in IP。

(2) GRE(General Routing Encapsulation,RFC 2784)。

(3) IPSec(IP Security)。

第二层隧道协议只能保证在隧道发生端及终止端进行认证及加密,而隧道在公网的传输过程中并不能完全保证安全。第三层隧道技术IPSec则是在隧道外面再封装,保证了隧道在传输过程中的安全性。下面将介绍第三层隧道协议,内容如下。

(1) IP中的IP(IP in IP)。IP in IP隧道由RFC 2003定义,规定了一种将整个IP(IPv4)包封装在另一个IP(IPv4)包中,前者为后者隧道载荷的方法。IP in IP规定外层的新IP头各字段设置如下。

① 版本号字段为4。

② 服务类型(TOS)字段直接从内部包的包头中复制。

③ 源地址和目的地址分别为隧道的入口和出口地址。

④ IP包头长度(IHL)、总长度和校验和需要重新计算。

⑤ 标记、标识和分片偏移量根据IP分片的相关标准进行。

⑥ 协议类型字段设置为4，表示载荷部分本身就是IPv4包(包括包头和载荷部分)。

⑦ 生存时间(TTL)字段设置为一个足够大的数值，以使封装后的包能够穿越网络到达隧道的出口。

如果IP包是被转发过来的，比如是通过某个物理端口进入隧道的，那么在隧道入口封装时，应将内部IP包头的生存时间递减并复制到外部包头。同样的，在去封装时，如果内部封装的IP包还需要转发，比如从隧道出口转发到某个物理端口，则它的生存时间字段也要做相应处理。

IP in IP的具体数据封装格式如图7-18所示。

<table>
<tr><th></th><th>0</th><th>4</th><th>8</th><th>16</th><th>19　　24　　31</th></tr>
<tr><td rowspan="5">新的IP头</td><td>版本号</td><td>包头长度</td><td>8位服务类型</td><td colspan="2">16位总长度</td></tr>
<tr><td colspan="3">16位标识</td><td>标志</td><td>13位片偏移</td></tr>
<tr><td colspan="2">8位生存时间</td><td>8位协议(=4)</td><td colspan="2">16位头校验和</td></tr>
<tr><td colspan="5">32位源IP地址(隧道入口地址)</td></tr>
<tr><td colspan="5">32位目的地址(隧道出口地址)</td></tr>
<tr><td rowspan="5">旧的IP头</td><td>版本号</td><td>包头长度</td><td>8位服务类型</td><td colspan="2">16位总长度</td></tr>
<tr><td colspan="3">16位标识</td><td>标志</td><td>13位片偏移</td></tr>
<tr><td colspan="2">8位生存时间</td><td>8位协议(=4)</td><td colspan="2">16位头校验和</td></tr>
<tr><td colspan="5">32位源IP地址(原始源地址)</td></tr>
<tr><td colspan="5">32位目的地址(原始目的地址)</td></tr>
<tr><td></td><td colspan="5">载荷数据(传输层报文)</td></tr>
</table>

图7-18　IP in IP的具体数据封装格式

(2) 通用路由封装协议(GRE)。GRE(Generic Routing Encapsulation，通用路由封装协议)由Cisco和NetSmiths公司于1994年提交给IETF，标号为RFC 1701和RFC 1702。2000年，Cisco等公司又对GRE协议进行了修订，称为GRE V2，标号为RFC 2784。目前，多数厂商的网络设备均支持GRE隧道协议。

GRE支持全部的路由协议(如RIP2、OSPF等)，用于在IP包中封装任何协议的数据包，包括IP、IPX、NetBEUI、AppleTalk、Banyan VINES、DECnet等。在GRE中，乘客协议就是上面这些被封装的协议，封装协议就是GRE，传输协议就是IP。GRE与IP in IP、IPX over IP等封装形式很相似，但它们更通用。在GRE的处理中，很多协议的细微差异都被忽略，这使得GRE不限于某个特定的"X over Y"应用，而是一种通用的封装形式。

GRE规定了如何用一种网络协议去封装另一种网络协议的方法。通过GRE，用户可以利用公共IP网络连接IPX网络、AppleTalk网络，还可以使用保留地址进行网络互连，或者对公网隐藏企业网的IP地址。GER只提供了数据包的封装，并没有加密功能来防止网络侦听和攻击，所以在实际环境中经常与IPSec在一起使用，由IPSec提供用户数据的加密，从而给用户提供更好的安全性。GRE隧道协议一般用在路由器中，可以满足内联网VPN以及外联网VPN的应用需求。

具体地说，路由器接收到一个需要封装和路由的原始数据包(比如IP包)，先在这个

载荷头
通用路由封装头
传送头

图 7-19　GRE 的封装原理

数据包的外面增加一个 GRE 头部，构成 GRE 报文，再为 GRE 报文增加一个 IP 头，从而构成最终的 IP 包。这个新生成的 IP 包完全由 IP 层负责转发，中间的路由器只负责转发，而根本不关心是何种乘客协议。以乘客协议 IP 为例，GRE 的封装原理和数据封装格式如图 7-19 和图 7-20 所示。

<table>
<tr><td></td><td colspan="5">0</td><td>4</td><td>8</td><td></td><td>16　19</td><td>24　31</td></tr>
<tr><td rowspan="5">新的IP头</td><td colspan="4">版本号</td><td colspan="2">包头长度</td><td colspan="2">8位服务类型</td><td colspan="2">16位总长度</td></tr>
<tr><td colspan="8">16位标识</td><td>标志</td><td>13位片偏移</td></tr>
<tr><td colspan="6">8位生存时间</td><td colspan="2">8位协议(=4)</td><td colspan="2">16位头校验和</td></tr>
<tr><td colspan="10">32位源IP地址(隧道入口地址)</td></tr>
<tr><td colspan="10">32位目的地址(隧道出口地址)</td></tr>
<tr><td rowspan="5">GRE头</td><td>C</td><td>R</td><td>K</td><td>S</td><td>S</td><td>Recur</td><td>标记</td><td>版本</td><td colspan="2">协议</td></tr>
<tr><td colspan="8">校验和(可选)</td><td colspan="2">偏移(可选)</td></tr>
<tr><td colspan="10">密钥(可选)</td></tr>
<tr><td colspan="10">序号(可选)</td></tr>
<tr><td colspan="10">路由(可选)</td></tr>
<tr><td rowspan="5">旧的IP头</td><td colspan="4">版本号</td><td colspan="2">包头长度</td><td colspan="2">8位服务类型</td><td colspan="2">16位总长度</td></tr>
<tr><td colspan="8">16位标识</td><td>标志</td><td>13位片偏移</td></tr>
<tr><td colspan="6">8位生存时间</td><td colspan="2">8位协议(=4)</td><td colspan="2">16位头校验和</td></tr>
<tr><td colspan="10">32位源IP地址(原始源地址)</td></tr>
<tr><td colspan="10">32位目的地址(原始目的地址)</td></tr>
<tr><td></td><td colspan="10">载荷数据(传输层报文)</td></tr>
</table>

图 7-20　GRE 的数据封装格式

利用 GRE 来进行 VPN 通信的原理如图 7-21 所示。

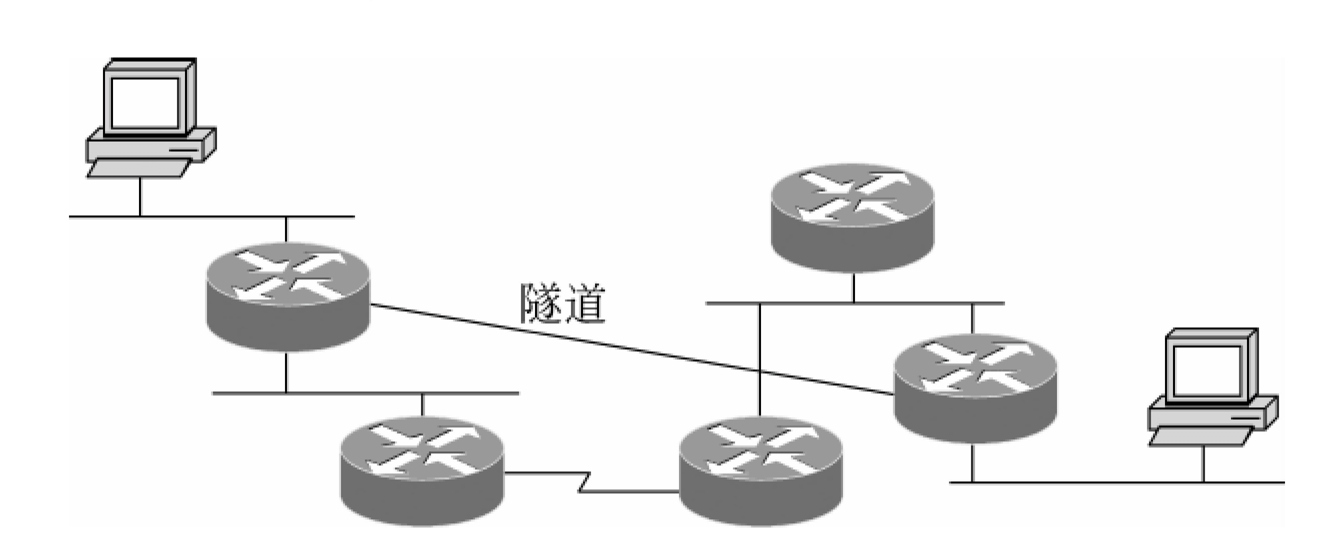


图 7-21　利用 GRE 实现 VPN

企业私有网络的 IP 地址通常是自行规划的保留 IP 地址，只是在企业网络出口有一个公网 IP 地址。原始 IP 数据包的 IP 地址通常是企业私有网络规划的保留 IP 地址，而外层的 IP 地址是企业网络出口的 IP 地址，因此，尽管私有网络的 IP 地址无法和外部网络进行正确的路由，但这个封装之后的 IP 包可以在 Internet 上路由。在接收端，将接收到包的 IP 头部和 GRE 头部解开后，将原始的 IP 数据包发送到自己的私有网络上，此时，私有网络上传输的 IP 包地址是保留 IP 地址，从而可以访问到远程企业的私有网络。这种技术是最简单的 VPN 技术。

GRE协议有如下优点。

① 通过GRE,用户可以利用公共IP网络连接非IP网络,如IPX网络、AppleTalk网络等。多协议的本地网可以通过单一协议的骨干网实现传输,比如两端的私有网络既有IP网,又有IPX等其他网络,通过GRE可以使所有协议的私有网络连接起来。

② 通过GRE,还可以使用保留地址进行网络互连,或者对公网隐藏企业网的IP地址。

③ 扩大了网络的工作范围,包括那些路由网关有限的协议。如IPX包最多可以转发16次(即经过16个路由器),而在一个隧道连接中,看上去只经过一个路由器。

④ GRE只提供封装,不提供加密,对路由器的性能影响较小,设备档次要求相对较低。

不过,由于GRE协议提出较早,也存在着如下一些缺点。

① GRE只提供数据包的封装,而没有加密功能来防止网络监听和攻击,所以在实际环境中,经常与IPSec一起使用。由IPSec提供用户数据的加密,从而给用户提供更好的安全性。

② 由于GRE与IPSec采用的是同样的基于隧道的VPN实现方式,所以IPSec VPN在管理、组网上的缺陷,GRE VPN也同样具有。

③ 同时,由于对原有IP报文进行了重新封装,所以同样无法实施IP QoS策略。

综上所述,GRE的优缺点可以看出,GRE VPN适合一些小型点对点的网络互连、实时性要求不高、要求提供地址空间重叠支持的网络环境。

(3) 三层隧道协议比较。第二层隧道和第三层隧道的本质区别在于用户的数据包是被封装在哪一层的数据包隧道里传输的。与第二层隧道相比,第三层隧道的优点在于它的安全性、可扩展性及可靠性。从安全的角度来看,由于第二层隧道一般终止在用户网设备(CPE)上,会对用户网的安全及防火墙技术提出较严峻的挑战。而第三层隧道一般终止在ISP的网关上,不会对用户网的安全构成威胁。从可扩展性角度来看,第二层IP隧道将整个PPP帧封装在报文内,可能会产生传输效率问题;其次,PPP会话会贯穿整个隧道,并终止在用户网的网关或服务器上。由于用户网内的网关要保存大量的PPP对话状态及信息,会对系统负荷产生较大的影响,当然也会影响系统的扩展性。除此之外,由于PPP的LCP(数据链路层控制)及NCP(网络层控制)对时间非常敏感,IP隧道的效率会造成PPP会话超时等问题。第三层隧道终止在ISP网内,并且PPP会话终止在RAS处,网点无须管理和维护每个PPP会话状态,从而减轻系统负荷。

对公司网络来说,第三层隧道技术还有一些其他优点。网络管理者采用第三层隧道技术时,不必在远程为客户原有设备(CPE)安装特殊软件。因为PPP和隧道终点由ISP的设备生成,CPE不用负担这些功能,而仅作为一台路由器。第三层隧道技术可采用任意厂家的CPE予以实现。使用第三层隧道技术的公司网络不需要IP地址,也具有安全性。服务提供商网络能够隐藏私有网络和远端结点地址。

一般来说,第二层隧道协议和第三层隧道协议分别使用,但合理地运用两层协议将具有更好的安全性。例如,L2TP与IPSec协议的配合使用可以分别形成L2TP VPN、IPSec VPN网络,也可以混合使用L2TP、IPSec协议,形成性能更强的L2TP VPN网络,

且这一VPN网络形式是目前性能最好、应用最广的一种,因为它能提供更加安全的数据通信,解决了用户的后顾之忧。表7-3为3种隧道协议在VPN中的性能比较。表7-4为PPTP、L2TP与IPSec这3种隧道协议在VPN中的性能比较。

表7-3　3种隧道协议在VPN中的性能比较

	GRE	IPSEC	MPLS
安全性	无	高	高,加密需另外协议支持
管理难易	对于组建大型VPN,较复杂	对于组建大型VPN,非常复杂	复杂
QoS保证	无,需要另外协议支持	无,需要另外协议支持	有
CPU负担	低	高	低
对网络要求	无特殊要求	无特殊要求	需要全部支持MPLS
不同厂家设备之间的互通性	容易	较困难	中等
是否需要虚拟路由器技术	是	是	是
适于运营商提供VPN服务	否,管理复杂	否,管理复杂,存在互通等问题	是

表7-4　PPTP、L2TP与IPSec隧道协议在VPN中的性能比较

协议选择	PPTP	L2TP	IPSec
网络模式	C/S	C/S	主机对主机的对等模式
使用方式	通过隧道进行远程操作	通过隧道进行远程操作	Internet、Extranet和通过隧道进行远程操作
OSI层	数据链路层	数据链路层	网络层
上层协议支持	IP、IPX等	IP、IPX等	IP
安全加密	MPPE加密技术	无标准(通常与IPSec一起组建VPN,所采用的加密技术也是由IPSec协议提供的,参考IPSec的加密技术)	DES和3DES
用户认证	采用PPP协议中的CHAP、MS-CHAP、MS-CHAPv2等验证方法	无标准(通常与IPSec一起组建VPN,所采用的用户身份验证技术也是由IPSec协议提供的,参考IPSec的用户认证技术)	AH
包认证	需要特殊解决	无标准	ESP
包加密	无标准	无标准	ISAKMP/Oakley、SKIP
密钥管理	无标准	无标准	IKE
隧道服务	单个点对点隧道,不能同时访问公用网	单个点对点隧道,不能同时访问公用网	多点隧道,同时访问VPN和公用网

3. 高层隧道协议

高层隧道协议是在网络层以上进行的，一般在传输层和会话层，或传输层与应用层之间，高层隧道协议有以下两种。

(1) SSL(Security Socket Layer)。

(2) Socks v5.0。

① SSL(Security Socket Layer)。

SSL VPN 的好处之一就是不需要安装客户端程序，远程用户可以随时随地从任何浏览器上安全接入到内联网络，安全地访问应用程序，无须安装或设置客户端软件，降低了企业的维护成本。因而，SSL 在点对网互连方面、在易用性和安全性上有着突出的优势。由于 SSL VPN 只适合点对网的连接，无法实现多个网络之间的安全互连，因此在企业组建网对网方面，IPSec VPN 就有着无可比拟的优势。详细对比如表 7-5 所示。

表 7-5 IPSec VPN 与 SSL VPN 的对比

选 项	SSL VPN	IPSec VPN
身份验证	单向身份验证、双向身份验证、数字证书	双向身份验证、数字证书
加密	强加密，基于 Web 浏览器	强加密，依靠执行
安全性	端到端安全，从用户到资源全程加密	网络边缘到客户端，仅对从用户到 VPN 网关之间通道加密
可访问性	可用于任何时间、任何地点访问	限制使用于已经定义好的受控用户的访问
费用	低(无须任何附加客户端软件)	高(需要管理客户端软件)
安装	即插即用安装，无须任何附加的用户软件、硬件安装	通常需要长时间的配置，需要客户端软件或硬件
用户的易使用性	对用户非常友好，使用非常熟悉的 Web 浏览器，无须终端用户的培训	对没有相应技术的用户比较困难，需要培训
支持的应用	基于 Web 的应用、文件共享、E-mail	所有基于 IP 的服务
用户	用户、合作伙伴用户、远程用户、供应商等	更适用于企业内部使用
可伸缩性	容易配置和扩展	在服务器容易实现自由伸缩，在客户端比较困难

② Socks(Protocol for Sessions Traversal Across Firewall Securely，防火墙安全会话转换协议)。目前一种流行的组网方式，就是利用防火墙，将企业内部网络和外部网络加以隔离。这种防火墙系统通常以应用层网关(Application Level Gateway，ALG)的形式工作在两个网络之间，提供 TELNET、FTP 以及 SMTP 等业务接入。随着越来越多应用层协议的出现，就有必要提供一个通用框架，来使应用协议安全而透明地穿过防火墙；其次，在实际应用中，还需要一种安全的认证方式，用以穿越防火墙。为了让客户/服务器应用程序方便，且安全地使用防火墙所提供的服务，Socks 协议(RFC 1928)设计了 TCP/UDP 之上的安全规程。从概念上来讲，该协议是位于应用层和传输层之间，向上层提供传输层的服务，不提供网络层网关的服务。

Socks v5 由 NEC 公司开发,工作在 OSI(Open System Internet)模型中的第 5 层——会话层,可作为建立高度安全的 VPN 基础。Socks v5 协议的优势在于访问控制,因此适用于安全性较高的 VPN。Socks v5 现在被 IETF(互联网工程任务组)建议作为建立 VPN 的标准,它的优点是能够非常详细地进行访问控制。即在网络层,只能根据源目的的 IP 地址允许或拒绝被通过,在会话层,控制手段更多一些;由于工作在会话层,能同底层协议,如 IPV4、IPSec、PPTP、L2TP 一起使用;用 Socks v5 的代理服务器,可隐藏网络地址结构;能为认证、加密和密钥管理提供"插件"模块,让用户自由地采用所需要的技术;Socks v5 可根据规则过滤数据流,包括 Java Applet 和 Actives 控制。当同 SSL 协议配合使用时,可用做企业的防火墙,防止黑客通过 Internet 对内部主机的未授权访问。但是,它也有不少令人遗憾之处:整体性能比低层次协议差,必须制定更复杂的安全管理策略,且推广时间较短,不如前面几种协议使用广泛。

7.8.2 加解密技术

VPN 利用 Internet 的基础设施传输企业私有信息。为了保证数据传输安全,对在公开信道上传输的 VPN 流量必须加密,以确保网络上未授权的用户无法读取信息。因此,可以说加解密技术是实现 VPN 的关键核心技术之一。加解密技术是数据通信中一项较成熟的技术,VPN 可直接利用现有技术。

大体上来说,加解密技术可以分为对称密钥加密和非对称密钥加密两类。另外,密钥管理也是非常重要的技术。

1. 对称密钥加密

对称密钥加密,也叫做共享密钥加密,是指加密和解密用的密钥是相同的,数据的发送者和接收者拥有共同的单个密钥。当要传输一段数据时,发送者利用密钥将其加密为密文,并在公共信道上传输,接收者收到密文后,也要用相同的密钥将其解密成明文。

比较著名的对称密钥加密算法有 DES 及其各种变形,比如 3DES、IDEA、RC4、RC5 等。众多算法中最常用的是 DES(Data Encryption Standard)、AES(Advanced Encryption Standard)和 IDEA(International Data Encryption Algorithm)。

由于加密和解密的密钥相同,因此这种加密算法的安全性取决于是否有未经授权的人获得了密钥。一旦密钥泄露,无论该算法在运行时多么复杂,设计多么精良,密文可以轻易被破解。为了保证密钥的机密性,使用对称密钥加密通信的双方,在交换加密数据之前必须先安全地交换密钥。

衡量对称算法优劣的一个重要尺度是密钥的长度。密钥位数越长,密钥的可能性越多,在找到正确密钥之前,必须测试的密钥数量就越多,从而破解这种算法就越困难。另一个指标,是看算法是否经得住算法分析的考验,如差分密码分析、线性密码分析等,有的算法密钥的长度虽然很长,但算法有缺陷,可绕过密钥进行破解。

对称密钥加密的优点是简单易用,易于用硬件实现,运算量小、速度快,适合于加密大量数据的情况;缺点是密钥的管理比较复杂。

2. 非对称密钥加密

非对称密钥加密使用两个密钥：公钥和私钥，这两个密钥在数学上是相关的。这种算法也叫做公钥加密。公钥可以不受保护，可在通信双方之间公开传递，或在公共网络上发布，但相关的私钥是保密的。利用公钥加密的数据只有使用私钥才能解密；利用私钥加密的数据只有使用公钥才能解密。

比较著名的非对称算法有 RSA、Diffie-Hellman、Rabin、椭圆曲线（ECC）、ElGamal 算法等。其中最有影响的是 RSA 算法，它能抵抗到目前为止已知的所有密码攻击。

非对称算法采用复杂的数学处理，密钥大小比对称算法的大，它们要求更多的处理器资源，因此速度较慢。非对称算法不适合加密大量数据的情况，而是经常用于关键数据的加密，比如对称密钥在密钥分发时采用非对称算法。另外，非对称加密算法和散列算法结合使用，可以生成数字签名。

非对称密钥加密的优点是解决了对称加密中密钥交换的困难，密钥管理简单，安全性高；缺点是计算速度相对较慢。因此，非对称密钥加密更多用于密钥交换、数字签名、身份认证等，一般不用于对具体信息加密。

一般来说，在 VPN 实现中，双方大量通信流量的加密使用对称加密算法，而在管理、分发对称加密的密钥上，采用更加安全的非对称加密技术。

7.8.3 密钥管理技术

密钥管理技术是 VPN 的另一项基础技术，它直接影响了各种加解密技术在 VPN 中的应用，也直接关系到 VPN 的安全，它的主要任务是在公用数据网上安全地传递密钥而不被窃取。密钥管理包括密钥的产生、分发、更改及销毁。目前，基于 IPSec 的密钥管理协议主要有 ISAKMP（Internet Security Association and Key Management Protocol，Internet 安全联盟和密钥管理协议，RFC 2408）、Oakley、IKE、Photuris、SKEME 和 SKIP（Simple Key Management for IP）等。在 IPSec 应用系统中，这 5 种协议都是使用 ESP 和 AH 来对 IP 数据包提供安全保护，并都需要专门的密钥管理信息包，以建立双方需要的密钥，然后才能进行安全通信。其中，ISAKMP、Oakley、IKE 还需要建立双方之间的安全关联。它们的优点是能提供较高的安全性，而且在以后的通信过程中不用携带密钥信息。但由于需要专门的密钥管理信息包，因此在突发事件中应变能力较差，特别是在密钥更新的过程中会带来通信的延迟。SKIP 主要是利用 Diffie-Hellman 的演算法则，在网络上传输密钥。

ISAKMP 和 IKE 协议详见第 3.5 节，本节将简要介绍 SKIP 协议。

SKIP 服务于无连接的数据包协议，如 IPv4 和 IPv6 的密钥管理机制，它是基于内嵌密钥的密钥管理协议。每个数据包都被一个密钥加密，这个密钥包含在数据包中，但同时又被另一个事先已被通信双方共享的密钥加密。SKIP 使用经过鉴别对方的公钥和自己的私钥来生成双方所共享的密钥，在每个 IPSec 通信包中都含有密钥信息。这样可以实现一包一密钥，随时进行密钥的更新。这不需要专门的密钥管理信息包，不会给通信带来

延迟，对于密钥更新非常快的宽带 VPN 环境下的应用特别有意义。例如，在吉比特 VPN 中，按照密钥管理策略的要求，若每 100Mbps 的传输数据就需要更新密钥，则每秒就需要更新一次密钥；若采用有连接状态的密钥管理协议，必然会频繁发送密钥管理信息包，如果密钥管理信息包丢失，就需要重传，这将大大影响通信效率；而采用无连接状态的密钥更新，则可以随时对密钥进行更新。若两个结点都已经有对方结点的公钥证书，则不需要额外的密钥交换包，因为到来的数据包中已经包含供接收结点计算共享密钥并且正确响应的足够信息。正是由于这个轻量级特点，当主机正与许多对等主机通信时，SKIP 对错误的恢复(如系统重启动)非常快。

需要指出的是，SKIP 并不提供回传保护(Back Traffic Protection，BTP)和完整转发安全性(Perfect-Forword Secrecy，PFS)。尽管它采用 Diffie-Hellman 密钥交换机制，但交换的进行是隐含的，也就是说，两个实体以证书形式彼此知道对方的 Diffie-Hellman 公钥，从而隐含地共享长期密钥。该长期密钥又可以导出，用来对随机产生的瞬时密钥进行加密的主密钥，而瞬时密钥才用来对 IP 包加密或鉴别。显然，一旦长期 Diffie-Hellman 密钥泄露，则任何在该密钥保护下的密钥所保护的相应通信都将被破解。而且 SKIP 是状态的，它支持一种称为在线密钥的概念，这个特性使得每个 IP 包可能是个别地进行加密和解密的，归根到底用的是不同的瞬时密钥。

SKIP 能有效应对中间人攻击、已知密钥攻击和拒绝服务攻击。SKIP 使用鉴别过的 Diffie-Hellman 公钥值，在获取通信对方公钥证书时，通过对发布证书的实体的数字签名进行验证，来对抗中间人攻击；而通过使用主密钥和瞬时密钥的两级密钥结构，SKIP 能对抗已知密钥(瞬时密钥)攻击；另外，SKIP 通过预先计算并缓存主密钥，可对抗拒绝服务攻击。

SKIP 的不足之处在于每个包都包含密钥信息，减少了每个包数据的传输量，每个包的传输效率变低。但对于高速环境，这种开销相对发送密钥交换包和丢包等造成的通信延迟而言，影响很小。在宽带 VPN 网络环境中，若采用 ISAKMP、Oakley、IKE、Photuris 或 SKEME 等密钥管理协议，必然会频繁发送密钥更新包。如果密钥更新包丢失，则需要重传，这将大大影响通信效率。而采用 SKIP，则可以随时对密钥进行更新，而无须发送专门的密钥管理信息包。因此，在宽带 VPN 环境下，国内外的发展趋势是尽量不采用像 ISAKMP、Oakley、IKE、Photuris 或 SKEME 等有连接状态的密钥管理协议，主要采用无连接状态的 SKIP 密钥管理协议。

7.8.4 VPN 身份认证技术

身份认证技术是一种用来验证通信双方是否真的就是他所声称的身份的手段。目前，通用的方法是使用数字证书或非对称密钥算法来鉴定用户的身份。通信双方交换资料前，必须首先向对方明示自己的身份，接着出示彼此的数字证书，再将证书进行比较，只有比较结果正确，双方才开始交换资料，否则不能进行后续的通信。

为了使 VPN 提供安全的信息传输功能，采用数据加密和认证技术是必不可少。"认证"是指验证一个最终用户或设备(如客户机、服务器、交换机、路由器或防火墙等)的

声明身份的过程，身份的认证往往与授权和访问控制密切相关。“授权”是指把访问权限授予一个用户、用户组或指定系统的过程，“访问控制”是指限制系统资源中的信息只能流到网络中的授权个人或系统，授权和访问控制往往都是伴随在成功的认证之后。在VPN中，用户身份认证技术是在正式的隧道连接开始前进行用户身份确认，以便系统进一步实施相应的资源访问控制和用户授权。

1. 安全口令

系统经常使用口令来认证用户或设备。为了避免口令被攻破，需要经常改变口令或加密口令。经常使用的口令生成方案有S/Key协议和令牌认证方案。

(1) S/Key协议。S/Key一次性口令系统是一种基于MD4和MD5的一次性口令生成方案。S/Key协议的运行是基于客户机/服务器的。客户机通过发送一个初始化包来启动S/Key交换，服务器用一个序列号和种子来响应。具体过程如下。

① 在准备阶段，客户机输入一个秘密口令字短语，这个口令字短语将与从服务器以明文传送形式传送的种子相连接。

② 对①生成的内容多次应用安全Hash函数，产生一个64位的最终输出。

③ 把一次性口令传送给服务器，在服务器上校验。

④ 服务器上相关文件存放了每个用户上一次成功登录时的一次性口令(如在UNIX上是/etc/skey/keys)。为了验证一次认证，认证服务器把接收到的一次性口令进行一次安全Hash函数运算。如果这个运算的结果与以前存储的一次性口令相匹配，则认证成功，并把接收的一次性口令存储起来，以供将来使用。使用一次性口令方案只能防止在初次登录到站点中时的重放攻击。如果需要保护的不仅是初始登录序列，则需要将一次性口令与其他形式的加密技术结合使用。

(2) 令牌认证方案。令牌认证系统通常要求使用一个特殊的卡，叫做“智能卡”或“令牌卡”，但也有一些地方可以用软件实现。这些类型的认证机制都是建立在“挑战—响应认证”和“时间—同步认证”两种方案之一的基础上。

2. PPP认证协议

点对点协议(Point-to-Point Protocol，PPP)是最常用的借助于串行线或ISDN建立拨入连接的协议。也正由于这点，它经常被用于VPN技术中。PPP认证机制包括口令认证协议(Password Authentication Protocol，PAP)、Shiva口令字认证协议(Shiva Password Authentication Protocol，SPAP)、可扩展认证协议(Extensible Authentication Protocol，EAP)和质询握手认证协议(Challenge Handshake Authentication Protocol，CHAP)。在所有这些情况中，认证的都是对等设备，而不是认证设备的用户。

(1) Shiva口令字认证协议SPAP。该协议是由Shiva公司发展的密码验证协议(PAP)的增强版本，是一种可逆加密机制。运行Windows 2000 Professional的计算机在连接到Shiva LAN Rover时会使用SPAP，就像Shiva客户机连接到运行Windows 2000的远程访问服务器一样。这种身份验证方式比明文身份验证更安全，但没有CHAP或MS-CHAP安全。

在启用 SPAP 作为身份验证协议时，同一用户密码总是以相同的可逆加密形式发送。这使得 SPAP 身份验证容易受到重放攻击。该攻击中有恶意的用户通过捕获身份验证过程数据包并重放响应，来获得对 Intranet 的身份验证访问。不鼓励使用 SPAP，特别是对虚拟专用网络连接。

优点：安全性较 PAP 好。

缺点：单向加密、单向认证，虽然是对密码进行加密，但还是会被破解，安全性差，通过认证后不支持 Microsoft 点对点加密(MPPE)。

(2) 可扩展认证协议 EAP。PPP 只能提供有限的验证方式。EAP 是由 IETF 提出的 PPP 协议的扩展，该协议允许那些使用任意长度的凭据和信息交换的任意身份验证方法。EAP 的开发是为了适应对身份验证方法日益增长的需求，这些身份验证方法使用其他安全设备并提供支持 PPP 内其他身份验证方法的工业标准结构。

通过使用 EAP，可以支持被称为 EAP 类型的许多特殊身份验证方案，其中包括令牌卡、一次性密码、使用智能卡的公钥身份验证、证书及其他方案。EAP(与强大的 EAP 类型一起)构成安全的虚拟专用网络 (VPN) 连接的重要技术组成部分。强大的 EAP 类型(例如那些基于证书的类型)在对抗野蛮攻击、词典攻击和密码猜测方面比基于密码的身份验证协议(如 CHAP 或 MS-CHAP)更加安全。

Windows XP 包括对两种 EAP 类型的支持：EAP-MD5 CHAP(等同于 CHAP 身份验证协议)和 EAP-TLS，用于基于用户证书的身份验证。最安全的认证方法就是和智能卡一起使用的"可扩展身份验证协议—传输层安全协议"，即 EAP-TLS 认证。

EAP-TLS 是一种双重身份验证方法，这意味着客户端和服务器都向对方证明自己的身份。在 EAP-TLS 交换过程中，远程访问客户端发送其用户证书，而远程访问服务器发送其计算机证书。如果其中一个证书未发送或无效，则连接终止。在 EAP-TLS 身份验证过程中，将为 Microsoft 点对点加密 (MPPE) 生成共享的机密加密密钥。

优点：安全性最好。

缺点：需要 PKI(公钥基础设施)支持(目前 PKI 还没有真正建立起来)。

3. 使用认证机制的协议

在给用户或设备提供授权和访问权限之前，许多协议需要认证校验。在 VPN 环境中，经常使用的是 TACACS 和 RADIUS(Remote Address Dial-In User Service)协议。它们提供可升级的认证数据库，并可采用不同的认证方法。

RADIUS 协议是一种访问服务器认证和记账协议，它在传输时使用 UDP。RADIUS 客户机通常是一个 NAS(网络访问服务器)，服务器是在 Unix 或 NT 机器上运行的监控程序。客户机负责把用户信息传递给指定的 RADIUS 服务器，然后对返回的响应进行操作，RADIUS 服务器负责接收用户连接请求。在 RADIUS 服务器中设立一个中心数据库，这个中心数据库包括用户身份认证信息(比如用户名、口令)。RADIUS 根据这个中心数据库来认证用户，然后返回客户机向用户提供服务所需要的全部配置信息。RADIUS 服务器可作为其他 RADIUS 服务器的代理，或作为其他类型认证服务器的客户机。RADIUS 服务器可支持多种方法来认证用户的身份，当把用户提交的用户名和初始口令

提供给服务器时，服务器可以支持PPP PAP、PPP CHAP、UNIX登录和其他认证机制。通常，用户登录由从NAS到RADIUS服务器的查询(Access Request)和服务器的相应响应(Access Accept或Access Reject)组成。Access Request包含了用户名、加密口令、NAS的IP地址和端口号。请求的格式还提供了用户想要的启动会话类型的信息。当RADIUS服务器从NAS接收到Access Request包之后，它将在数据库中搜索所列出的用户名。如果数据库中不存在此名，则将加载一个默认的配置文件，或立即发送一条Access Reject消息。RADIUS的认证和授权功能是相互结合在一起的，如果找到了用户名并且口令正确，RADIUS服务器会返回一个Access Accept响应，包含用于该次会话的参数属性和值的列表。

客户机与RADIUS服务器之间的事务是通过使用共享密钥来认证的，这个密钥从不在网络上发送。在客户机与服务器之间的任何用户口令都必须以加密方式发送，以消除有人在不安全网络上窃听，从而确定用户口令的可能性。加密是在RADIUS客户机与RADIUS服务器之间实施的，如果RADIUS客户机是一个NAS，而不是客户机PC，则PC和NAS之间的任何通信都没有加密。

4. 数字签名技术

在VPN安全保密系统中，数字签名技术有着特别重要的地位，VPN网络安全服务中的源鉴别、完整性服务及不可否认服务等，都要用到数字签名技术。在VPN中完善的数字签名应具备签字方不能抵赖、他人不能伪造和在公证人面前能够验证真伪的能力。

习题7

一、填空题

可以采用________、________和________协议实现VPN网络。

二、选择题

1. 不适合采用VPN的情况是________。
   A. 位置众多，特别是单个用户和远程办公室站点多，例如企业用户、远程教育用户
   B. 用户/站点分布范围广，彼此之间的距离远，遍布全球各地，需通过长途电信，甚至国际长途手段联系的用户
   C. 对线路保密性和可用性有一定要求的用户
   D. 不管价格多少，性能都被放在第一位的情况
2. 目前，VPN使用了________技术，保证了通信的安全性。
   A. 隧道协议、身份验证和数据加密　　B. 身份验证、数据加密
   C. 隧道协议、身份验证　　D. 隧道协议、数据加密

3. VPN 的英文全称是________。

A. Visual Protocol Network　　B. Virtual Private Network

C. Virtual Protocol Network　　D. Visual Private Network

4. PPTP、L2TP 和 L2F 隧道协议属于________。

A. 第一层隧道　　B. 第二层隧道

C. 第三层隧道　　D. 第四层隧道

5. 下列选项中的________不属于 VPN 的缺点。

A. 尽管 VPN 的设备供应商们可以为远程办公室或 Extranet 服务的专线或帧中继提供有效方式，可是 VPN 的服务提供商们只保证数据在其管辖范围内的性能，一旦出了其“辖区”，则安全没有保证

B. VPN 用户的增加和删除只是逻辑的操作，无须专门的物理设备和连接

C. 不同厂商的 VPN 管理和配置掌握起来是最难的，这还需要同时熟悉不同厂商的执行方式

D. 作为一种典型技术，VPN 的应用时间还不长，VPN 的管理流程和平台相对于其他远程接入服务器或其他网络结构的设备来说，有时并不太好用

6. 一套完整的 VPN 产品一般包括________部分。

A. VPN 网关、VPN 客户端、VPN 管理中心和防火墙

B. VPN 网关、VPN 客户端

C. VPN 网关、VPN 管理中心

D. VPN 网关、VPN 客户端、VPN 管理中心

7. 不属于 VPN 的核心技术是________。

A. 隧道技术　　B. 身份验证

C. 日志记录　　D. 访问控制

三、简答题

请说出 SSL VPN 与 IPSec VPN 网络的区别。

第 8 章　VPN 的应用案例

本章重点描述了一些现实工作中遇到的工程问题，按照一个工程实施的基本步骤，对其进行需求分析、方案确定，并最终配置实施，实施过程中的配置环节是本章关注的重点。

下面以 A 公司和高校的应用来讲述 VPN 的应用模式。假设随着 A 公司分支机构和用户群的不断扩大，要保证分支机构、合作伙伴以及移动用户对中心电子商务资源的不间断以及大数据量的访问，确保授权用户只能在授权场所才能够进行数据访问；同时降低经营成本，最大程度使用现有资源，有效压缩各项费用。本章着重介绍 A 公司与分支机构之间的内联网 VPN，A 公司与合作伙伴之间的外联 VPN 和高校与移动用户之间的远程拨入 VPN 应用实例及配置流程。

8.1　企业内部虚拟网

企业内部虚拟网（Intranet VPN）是指同一个机构内部的多个网络站点位于不同的地理位置，每个站点都有多个 IP 子网，VPN 被用来连接这些站点，从而形成一个更大的企业内部互联网络，简称内联网。

8.1.1　A 公司 VPN 部署总体框架

1. A 公司 VPN 部署案例背景介绍

A 公司已经在上海和北京建成了以以太网技术为核心的局域网，不少分支机构也有自己以太网络。现在，全国各地的营业所目前采用在用户自己的 PC 上安装 ISDN TA 卡的方式，通过 ISDN 拨号访问到总部的 Cisco 拨号访问服务器，进而访问局域网内的数据资源。

2. 该案例需求分析

按照 A 公司的情况，在北京和上海的公司都有自己的以太网，而公司领导非常期望能使其成为跨区域的局域网（实际应用中通常不建议这样做，一般只对少数服务跨区域提供，如 VoIP）。由于在全国各地分布营业所，要求北京总部需要在硬件支持的最大并发用户数大于或等于 2500 用户，而且全国分布的营业所是固定的，连入本地的 ISP。

为了突出本章所关心的内容，对 A 公司现有网络结构进行简化，形成了如图 8-1 所示的 A 公司现有网络结构简图。

3. 技术方案确定

这是个典型的 L2L（LAN to LAN）应用，而路由器通常是 L2L 会话的最好解决方

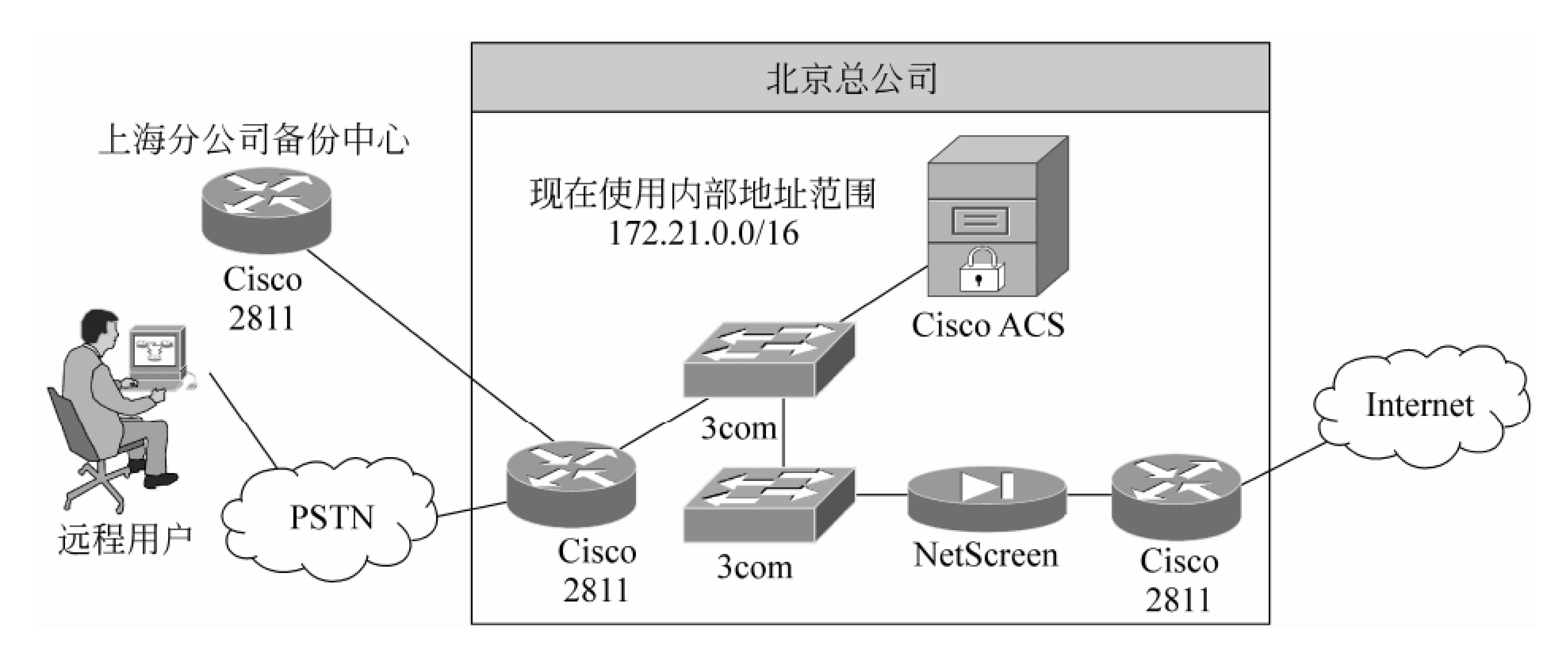


图 8-1　A 公司现有网络结构简图

案，它支持路由选择。

技术路线：根据需求，采用企业内部虚拟网(Intranet VPN)。

设备选择：北京和上海总部的 2811 系列路由器可以继续使用，各分支机构新购买 1811 系列路由器来实施。

地址规划：营业所的局域网需要通过 VPN 访问总部局域网，因此需要对 A 公司总部和分支机构的局域网地址进行统一规划分配，这样才能够正常通信。

总部内部的局域网现在已经正常运行，由于该公司网络建设初期有良好的设计，使得地址分配非常容易，北京公司的内部 IP 地址范围为 172.21.0.0/16，上海使用了 172.22.0.0/16 的地址段。对于全国各地的营业所，需要从由 RFC 1918 所定义的私有 IP 地址范围内选择合适的 IP 地址，唯一地分配给营业所。根据用户的规模，选择已经使用的 172.16.0.0/16 为 A 公司全国营业所的局域网 IP 地址范围。

根据营业所用户的规模，可以分配一个 C 类的网络给一个营业所的局域网使用。例如，分配 172.16.1.0/24 给第一个营业所使用，以此类推。这样，172.16.0.0/16 可以最多支持 256 个分支机构，当前和未来都能够很好地满足 A 公司的发展规模。

改造升级后的网络结构简图如图 8-2 所示。

8.1.2　路由器站点到站点连接

为了完成路由器站点到站点的 VPN，回顾前面学习的基本原理相关内容，并对实际使用的命令进行解释。使用 ISAKMP/IKE 路由器站点到站点的 VPN 配置，首先是对 ISAKMP/IKE 阶段 1 的配置，然后是 ISAKMP/IKE 阶段 2 的配置。

1. ISAKMP/IKE 阶段 1 的配置

对于阶段 1，包含协商阶段 1 的策略制定、设备验证。

(1) 策略的制定又包含优先权、加密算法、散列算法、验证算法、DH 组和连接的生存周期。

参考思科公司 IOS 的 Command References 文档，策略制定所包含的步骤依次表示

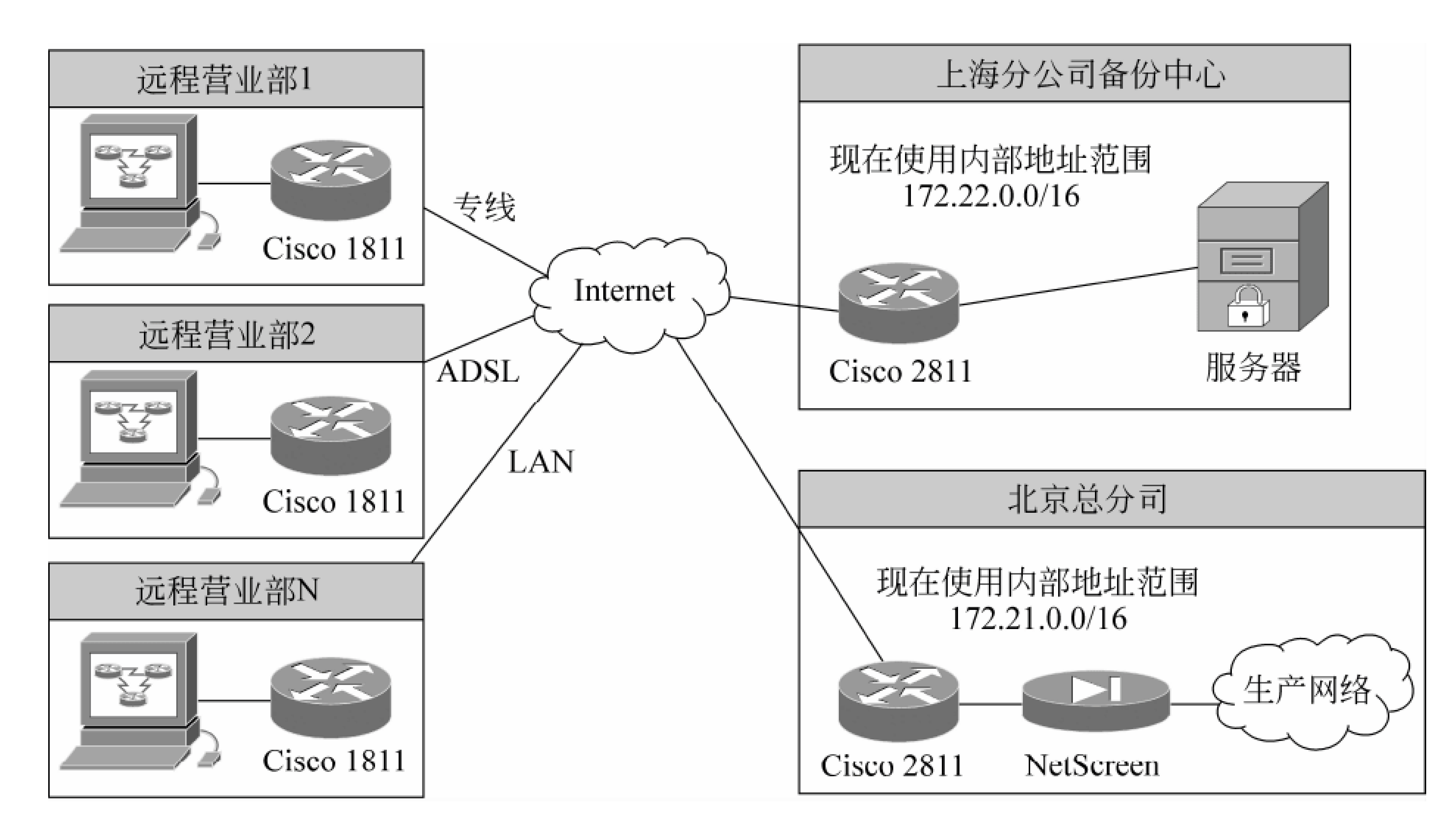


图 8-2 A 公司升级后的网络结构简图

如下：

```
Router(config)#cypto isakmp policy priority
Router(config-isakmp)#encryption {des|3des|aes}
Router(config-isakmp)#hash {sha|md5}
Router(config-isakmp)#authentication {rsa-sig|rsa-encr|pre-share}
Router(config-isakmp)#group {1|2|5}
Router(config-isakmp)#lifetime seconds
```

各项的默认值设置如下：

```
encryption(IKE policy);default=56-bit DES-CBC
hash(IKE policy);default=SHA-1
authenticaion;default=RSA signatures
group(IKE policy);default=768-bit Diffie-Hellman (即 DH 组默认为 1)
lifetime(IKE policy);default=86,400 seconds (one day)
```

(2) 思科路由器验证 IPSec 设备支持 3 种方法：预共享密钥、RSA 加密随机数和 RSA 签名(或叫做数字证书)。

参考思科公司 IOS 的 Command References 文档，预共享密钥配置表示如下：

Router(config)# crypto isakmp *key key*-string address peer-address[*mask*][no-xauth]

注意： 当同一台路由器同时存在 L2L(如站点到站点的 VPN)和远程访问(如 Easy VPN)的会话，路由器将用 XAUTH(用户验证，需要提供用户名和密码)为两种连接执行认证，而 L2L 是共享密钥，没有用户名和密码，这样对于 L2L 的会话就会产生问题，连接将会失败。因此，建议用户无论是否有远程访问(Easy VPN)的会话，都应该配置 no-xauth 参数，即 L2L 不使用发送用户名和密码来做认证，但是远程访问还是试图用 XAUTH。

对于 RSA 加密随机数和 RSA 签名(或叫做数字证书),本书不具体介绍。请参考思科相关文档。

RSA 随机数配置分为两步,内容如下。

第 1 步:在每一台对等设备上产生 RSA 加密随机数(公钥和私钥),对于每一台远端的对等设备,可以产生不同的公钥/私钥。

第 2 步:在所有对等设备上共享公钥,并配置对等设备的公钥。

RSA 签名配置分为 6 步,内容如下。

第 1 步:配置主机名和域名。

第 2 步:产生一个 RSA 密钥对。

第 3 步:定义一个证书授权或 CA。

第 4 步:下载和验证 CA 的证书。

第 5 步:请求路由器的身份证书。

第 6 步:存储 CA 和身份证书。

2. ISAKMP/IKE 阶段 2 的 L2L 会话配置

阶段 2 的 L2L 会话有 3 个方面:定义需要被保护的流量,定义流量是如何被保护的,定义流量应该转发给谁。

(1) 定义需要被保护的流量。定义被保护流量的一种方法就是建立一个 crypto ACL,即带有 permit 或者 deny 语句的 ACL 条目组。permit 语句指定了需要被保护的流量,deny 指定了不需要被保护的流量。由于 VPN 是端到端的流量保护,所以应该采用扩展的访问控制列表来表示。这就需要保证两边访问控制列表的一致性,使得本地被保护流量能够正确地被对等设备处理,反之亦然。

注意: 如果为了图省事,没有配置 crypto ACL,大多数情况下,ISAKMP/IKE 阶段 2 的连接会失败。如果只配置 permit any any,也可能出现意想不到的问题。

例如北京总公司和上海分公司的 crypto ACL 应该如下:

北京总公司配置:

```
Router(config)#ip access-list extended mirrored
Router(config-ext-nacl)#permit ip 172.21.0.0 0.0.255.255
                                   172.22.0.0 0.0.255.255
```

上海分公司配置:

```
Router(config)#ip access-list extended mirrored
Router(config-ext-nacl)#permit ip 172.22.0.0 0.0.255.255
                                   172.21.0.0 0.0.255.255
```

(2) 定义流量的保护方法:Transform Sets(传输集)。crypto ACL 定义了需要保护的流量,传输集定义了数据流量是如何被保护的。一个传输集包含安全协议、使用的算法。ISAKMP/IKE 阶段 2 的连接要建立,必须在对等路由器两方有至少一个匹配的传输集。建立传输集的命令如下:

```
Router(config)#crypto ipsec transform-set transform-set-name
```

```
transform1[transform2][transform3][transform4]
```

配置参数说明如下：

transform-set-name	创建的传输集名称
transform1	认证头部 Authentication Header(AH)
transform2	ESP 加密 Encapsulating Security Payload(ESP)encryption
transform3	ESP 认证 ESP authentication
transform4	压缩算法 compression

(3) 使用 Crypto Map 定义流量转发给谁。通过 crypto map，将所有必要信息组织在一起，构成一个 IPSec 会话。crypto map 有两种类型：静态的 crypto map 和动态的 crypto map。静态的 crypto map 通常用于 L2L 会话，动态的 crypto map 用于远程访问。当然，动态的 crypto map 也可以用于 L2L 的会话，但是不推荐这么使用。

crypto map 的配置步骤包含 crypto map 中的条目确定、使用 ISAKMP/IKE 来构建 IPSec 数据连接或手动建立连接、激活一个 crypto map 条目等。

对等的两台路由器上必须有兼容的 crypto map 中的条目，而这个条目至少含有一个 crypto ACL、一个匹配的对等设备身份和一个一致的传输集。

只有 1%的时候使用手动建立连接的方法，故本文不介绍手动建立连接的方法，即不介绍不使用 ISAKMP/IKE 来建立连接的方法。使用 ISAKMP/IKE 来构建 IPSec 数据连接，建立一个静态的 crypto map 条目，使用如下配置：

```
Router(config)#crypto map map-name seq-num[ipsec-isakmp]
                 [dynamic dynamic-map-name][discover][profile profile-name]
Router(config-crypto-m)#match address[access-list-id|name]
Router(config-crypto-m)#set peer {host-name[dynamic][default]|
                            ip-address[default] }
Router(config-crypto-m)#set transform-set transform-set-name
```

crypto map 的配置远远不止上面提到的命令，但是上面提到的命令是必须配置的。这些命令的具体含义如下：

match address(IPSec)	需要匹配 crypto ACL 的名字或号码
set peer(IPsec)	与自己相连的一个 IPsec 对等设备，可以为 IP 或域名
set transform-set	指定使用的传输集名字

crypto map 建立一条静态的映射条目，后面跟一个唯一的名字，名字后面有一个序列号，最小为 1，最大为 65535，序列号越小，语句的优先级越高。因为使用 ISAKMP/IKE，后面必须有 ipsec-isakmp 关键字。采用静态的 crypto map，后面其他选项就不用配置。相关内容请参看思科命令参考文档。

输入第一条命令后，将进入一个子命令模式，上面所列的为必须配置的命令。match address 命令指定了保护流量的静态 crypto ACL 的名字或号码。set peer 静态地指定对等设备，如果指定对等设备的名字，就需要用 DNS 或静态主机列表来解析它。用户可以同时写多条对等设备命令(通常是冗余的需要)，但是只有一台设备能够建立连接。set

transform-set 静态地制定所使用的传输集名字，用于保护去网 set peer 命令中对等设备的流量。也可以同时配置多个传输集，但是要注意对等设备传输集的一致性。

还有其他一些可选命令，请参看下面思科命令参考文档相关内容：

```
set pfs Specifies that IPsec should ask for PFS when requesting new SAs for this
crypto map entry,or that IPsec requires PFS when receiving requests for new SAs.
set security-association level per-host Specifies that separate IPsec SAs should be
requested for each source/destination host pair.
set security-association lifetime Overrides(for a particular crypto map entry)the
global lifetime value,which is used when negotiating IPsec SAs.
set session-key Specifies the IPsec session keys within a crypto map entry.
```

最后，还需要把这个 crypto map 激活，才会去保护流量。用户可以选择和对等设备相连接的物理接口上激活它，也可以选择一个非物理接口激活。一般在物理接口上配置激活，有如下配置：

```
router(config)#interface type[slot_#]port_#
router(config-if)#crypto map map_name
```

进入路由器的接口模式后，用 crypto map 命令把前面指定的静态 crypto map 应用到路由器的接口上。

3. 站点到站点连接总结

经过上面两步的配置，一个站点到站点连接就基本完成了。可以通过一些 show 命令来检查所做的配置，或者通过 sniffer 软件抓包来验证。

当然，也可以通过 debug 相关命令进行查看，使用时需要注意此命令对路由器 cpu 以及内存资源的影响。

对于使用数字证书验证设备、动态的 crypto map、基于名字的 crypto map 等技术，这里没有进行详细介绍，需要参看思科命令参考文档以及思科配置指南文档。

建立和使用 L2L 会话时，可能还需要处理其他一些问题，如需要做地址转换(NAT 或 PAT)、QoS、非单播流量的应用、路由协议的使用等。

8.1.3 案例实施(路由器站点到站点连接配置)

由于选择了一个简单可行的技术方案，加上前面的技术准备非常充分，实施起来就比较容易。

思科路由器的配置，除了使用命令行模式配置外，还可以采用 SDM 软件配置，而且使用 SDM 软件配置会容易得多。本文继续讨论使用命令行模式来配置 VPN，使用 SDM 的方法不再介绍。

1. 实施前的准备工作

实施前，用户需要考虑清楚要准备什么或者亲自做一下实验，来确定自己的想法，不

要盲目地操作。比如确定现在路由器的配置,并需要对现有的配置备份、确定路由器的物理位置、确定要使用的跳线是否准备妥当、确定 IOS 是否能够完全满足当前需求、确定配置切换时间等。

必须记住工程实施前要考虑的各种问题,甚至要考虑这次施工可能达不到预期效果或者使网络变得很糟糕(本次施工是进行网络改造,而不是新建,所有分支机构也不可能一次完成),需要做一个回退的方案。

一个工程的成功与否,不仅取决于是否掌握了前面的技术细节问题,还需要有一个明确可行的实施计划。

由于这些问题不是本文讨论的重点,就不再赘述。

本次实施简要分为 4 步,上海分支机构 ISAKMP/IKE 阶段 1 和阶段 2 的配置;北京本部 ISAKMP/IKE 阶段 1 和阶段 2 的配置;路由协议的使用的配置;检查与验证配置。

2. 上海分支机构到北京总部的 ISAKMP/IKE 阶段 1 和阶段 2 的配置

基本配置:如路由器命名为 ShangHai 和 ISP 互联的地址配置,以及连接用户的地址配置,到 ISP 的静态路由等,不再赘述。

阶段 1 策略制定配置如下:

```
ShangHai#configure terminal
ShangHai(config)#crypto isakmp policy 1
ShangHai(config-isakmp)#encr 3des
ShangHai(config-isakmp)#hash md5
ShangHai(config-isakmp)#authentication pre-share
ShangHai(config-isakmp)#group 2
```

阶段 1 的共享密钥设备验证配置如下:

```
ShangHai(config)#crypto isakmp key cisco123 address 10.1.1.2 no-xauth
```

上面制定了一个典型的阶段 1 策略,并使用预共享密钥来验证设备。

阶段 2 的传输集配置如下:

```
ShangHai(config)#crypto ipsec transform-set ShangHai esp-3des esp-md5-hmac
```

使用 ISAKMP/IKE,建立一个阶段 2 的 crypto map 条目,配置如下:

```
ShangHai(config)#crypto map ShangHai_MAP 1 ipsec-isakmp
ShangHai(config-crypto-m)#set peer 10.1.1.2
ShangHai(config-crypto-m)#set transform-set ShangHai
ShangHai(config-crypto-m)#match address mirrored
```

定义需要保护的流量,配合 cryto map 使用,配置如下:

```
ShangHai(config)#ip access-list extended mirrored
ShangHai(config-ext-nacl)#permit ip 172.22.0.0 0.0.255.255 172.21.0.0 0.0.255.255
```

这样,上海分公司的 VPN 配置基本完成,最有需要在和 ISP 连接的端口上应用,配

置如下：

```
ShangHai(config)#interface FastEthernet0/1
ShangHai(config-if)#ip address 10.2.2.2 255.255.255.252
ShangHai(config-if)#crypto map ShangHai_MAP
```

3. 北京总部对上海分支机构的 ISAKMP/IKE 阶段 1 和阶段 2 的配置

阶段 1 策略制定配置如下：

```
BeiJing(config)#configure terminal
BeiJing(config)#crypto isakmp policy 1
BeiJing(config-isakmp)#encr 3des
BeiJing(config-isakmp)#hash md5
BeiJing(config-isakmp)#authentication pre-share
BeiJing(config-isakmp)#group 2
```

阶段 1 的共享密钥设备验证配置如下：

```
BeiJing(config)#crypto isakmp key cisco123 address 10.2.2.2 no-xauth
```

阶段 2 的传输集配置如下：

```
BeiJing(config)#crypto ipsec transform-set BeiJing esp-3des esp-md5-hmac
```

使用 ISAKMP/IKE，建立一个阶段 2 的 crypto map 条目，内容如下：

```
BeiJing(config)#crypto map BeiJing_MAP 1 ipsec-isakmp
BeiJing(config-crypto-m)#set peer 10.2.2.2
BeiJing(config-crypto-m)#set transform-set BeiJing
BeiJing(config-crypto-m)#match address mirrored
```

定义需要保护的流量，配合 cryto map 使用，配置如下：

```
BeiJing(config)#ip access-list extended mirrored
BeiJing(config-ext-nacl)#permit ip 172.21.0.0 0.0.255.255 172.22.0.0 0.0.255.255
```

在和 ISP 连接的端口上应用配置如下：

```
BeiJing(config)#interface FastEthernet0/1
BeiJing(config-if) #ip address 10.1.1.2 255.255.255.252
BeiJing(config-if) #crypto map BeiJing_MAP
```

4. 北京总部和上海分支机构的路由配置

前面的配置仅仅完成了 VPN 的互联，而该项目还需要一个内部路由。对于在异地的公司，需要运行内部的路由协议，该怎么办呢？经过 VPN 的配置，大家也许想到使用 VPN 来做，只有 VPN 才能把两边互联起来，而且看起来像一个内部网络。如果在上面能够运行路由协议，问题解决。但是站点到站点的 IPSec VPN 是一个问题，它只支持单播

流量;组播和广播流量是不能穿越的,即不支持路由协议。

前面简单介绍过,GRE 是一个 3 层的传输协议,它允许将其他的协议,例如 IP、IPX、AppleTalk 等协议,封装在一个不同的 IP 单播数据包。如果利用 GRE,将一个组播或广播数据包封装在一个单播数据包中,这样 IPSec 就可以处理了。

GRE 隧道的配置是一件相当简单的事情,包含以下配置:

```
定义隧道接口: interface Tunnel
隧道数据包的源 IP 地址: tunnel source
隧道数据包的目的 IP 地址: tunnel destination
还有一些可选的配置,如隧道封装方法;Keepalive 等
```

根据上面的介绍,在上海 GRE 隧道的配置如下:

```
ShangHai(config)#interface Tunnel0
ShangHai(config-if)#ip address 172.31.1.2 255.255.255.0
ShangHai(config-if)#tunnel source 10.2.2.2
ShangHai(config-if)#tunnel destination 10.1.1.2
```

上海动态路由协议的配置如下:

```
ShangHai(config)#router ospf 1
ShangHai(config-router)#network 172.22.0.0 0.0.255.255 area 2
ShangHai(config-router)#network 172.31.1.0 0.0.255.255 area 0
```

北京 GRE 隧道的配置如下:

```
BeiJing(config)#interface Tunnel0
BeiJing(config-if)#ip address 172.31.1.1 255.255.255.0
BeiJing(config-if)#tunnel source 10.1.1.2
BeiJing(config-if)#tunnel destination 10.2.2.2
```

北京动态路由协议的配置如下:

```
BeiJing(config)#router ospf 1
BeiJing(config-router)#network 172.21.0.0 0.0.255.255 area 1
BeiJing(config-router)#network 172.31.1.0 0.0.0.255 area 0
```

这样就可以通过 OSPF 路由协议,把分支机构和上海总部连接起来了。

5. 验证配置

用户可以通过一些常用的命令来检查配置结果是否符合之前的预想。第 1 步看 VPN 是否成功建立,即根据访问控制列表,制造一些需要加密的流量,把这些流量发到对端,并通过 show crypto engine connections active 查看加密和解密的数据包情况,内容如下:

```
ShangHai #show crypto engine connections active
Crypto Engine Connections
```

```
  ID  Type    Algorithm     Encrypt  Decrypt     IP-Address
1001  IKE     MD5+3DES            0        0     10.1.1.2
1002  IKE     MD5+3DES            0        0     10.1.1.2
2003  IPsec   3DES+MD5            0      270     10.1.1.2
2004  IPsec   3DES+MD5          269        0     10.1.1.2
```

要验证阶段 1 策略制定情况，用 show crypto isakmp policy 命令，内容如下：

```
ShangHai#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
    encryption algorithm:    Three key triple DES
    hash algorithm:          Message Digest 5
    authentication method:   Pre-Shared Key
    Diffie-Hellman group:    #2(1024 bit)
    lifetime:                86400 seconds,no volume limit
Default protection suite
    encryption algorithm:    DES-Data Encryption Standard (56 bit keys)
    hash algorithm:          Secure Hash Standard
    authentication method:   Rivest-Shamir-Adleman Signature
    Diffie-Hellman group:    #1(768 bit)
    lifetime:                86400 seconds,no volume limit
```

用户还可以利用 show crypto map 以及 show crypto ipsec transform-set 来查阶段 2 的一些配置，内容如下：

```
ShangHai#show crypto map
Crypto Map ShangHai_MAP 1 ipsec-isakmp
    Peer=10.1.1.2
    Extended IP access list mirrored
        access-list mirrored permit ip 172.22.0.0 0.0.255.255 172.21.0.0 0.0.255.255
        access-list mirrored permit ip host 10.2.2.2 host 10.1.1.2
    Current peer: 10.1.1.2
    Security association lifetime: 4608000 kilobytes/3600 seconds
    PFS(Y/N): N
    Transform sets=
    {
            ShangHai,
    }
    Interfaces using crypto map ShangHai_MAP:
            FastEthernet0/1
```

掌握上述命令后，用户利用 show crypto ipsec sa 还可以获取更进一步的信息。

show ip route ospf 可以检测 ospf 是否成功建立，内容如下：

```
ShangHai#show ip route ospf
    172.21.0.0/24 is subnetted,1 subnets
        172.21.4.0[110/1001]via 172.31.1.1,00:00:17,Tunnel0
```

6. 对该案例的一些思考

是不是到此就结束了呢？这样对用户来说已经能正常使用了，但是还有一些有用的问题值得大家思考。

首先，本案例的 ISP 使用的地址是私有地址，实际项目中却不这么简单。我们都知道，这些私有地址是无法在互联网路由的，而且一个公司的地址可能是一个或几个公网地址，这就涉及需要做 NAT 的问题。既要做 NAT 又要做站点到站点的 VPN。

其次，在通过 GRE 解决非单播流量的问题时，crypto map 是否必须用在物理接口，能否用在 GRE 通道的 tunnel 接口呢？有什么不同？

最后，IPSec 的 HSRP 冗余问题。假设有一种拓扑，总部办公室出口用了两台路由器，并且运行 HSRP 协议，而分支机构要和总部建立站点到站点的 IPSec VPN。

在实际项目中，这些问题是经常遇到的，读者可以参看思科的相关文档，解决上述问题。

8.2 企业外部虚拟网

如果一个 VPN 配置实例中的所有站点都属同一个企业，这个 VPN 配置实例就是一个公司内联网。如果分属不同企业，该 VPN 配置实例就是企业外部虚拟网（Extranet VPN），简称外联网。一个站点可在多个 VPN 配置实例中，如一个内联网和多个外联网中。内联网和外联网都视做 VPN 配置实例。一般而言，VPN 配置实例并不区分内联网或外联网，它们都属于站点到站点的连接，因此技术实现也非常相似。本例对上述 A 公司案例进行一些扩展和探讨。

外联网为许多公司提供了方便，让公司可以向供应商、客户、合作伙伴开放自己的网络，支持实时协作。如果与外部人员共享的系统数量少，这些系统上的授权级别又能得到严格控制，外联网（如 IPSec、SSL 和远程桌面）的使用效果会相当好。但是，外联网也可能会成问题，因为也许要访问多个系统，或者必须授予接入者高级别的权限，公司常常无意中授予访问者过大的访问权，而访问活动也无法受到密切监视及控制。

8.2.1 A 公司 VPN 部署框架

前面对 A 公司站点到站点的内联网 VPN 进行介绍。现在由于 A 公司的业务继续扩展，要与一些公司进行业务共享、财务结算等业务，出于安全性考虑，A 公司和商业伙伴需要利用 VPN 进行连接，即外联网的 VPN。

根据这一需求的变化，公司 A 的对外业务服务器放在了上海，新的网络结构简图如图 8-3 所示。

上海分公司和北京总公司的内联网 VPN 不再介绍，主要对商业合作伙伴与上海分公司的连接进行介绍。图 8-3 中，上海分公司的服务器为专用的商业合作使用。具体地

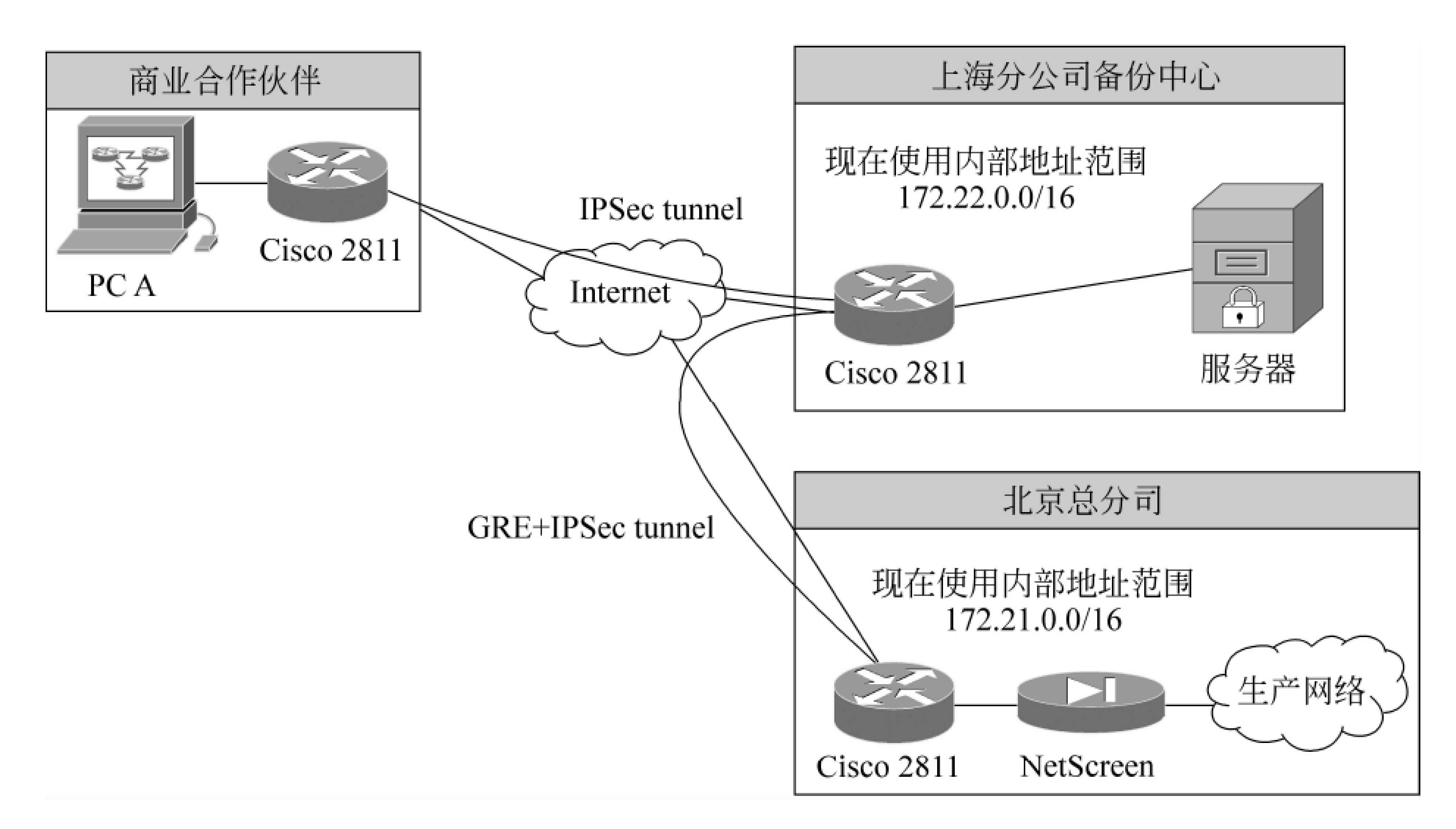


图 8-3　A 公司与商业合作伙伴的网络结构简图

址规划如表 8-1 所示。

表 8-1　网络地址规划

公司 A 上海分公司			商业合作伙伴		
硬件	Internet 连接接口地址	公司内部接口地址	硬件	Internet 连接接口地址	公司内部接口地址
Cisco 2811	Fast Ethernet1/110.2.3.2/30	Fast Ethernet1/2172.22.90.254/24	Cisco 2811	Fast Ethernet1/110.3.3.2/30	Fast Ethernet1/2192.168.1.254/24
服务器		172.22.90.1/24	PC A		192.168.1.1/24

8.2.2　外联网 VPN

前面介绍外联网 VPN 和内联网站点到站点 VPN 实现的不同点在于外联网 VPN 的访问控制、安全策略。本例中，可以对在连接服务器的路由器上配置一些安全特性，更好地保护服务器，最好把服务器单独放在一个区域。

1. 路由器站点到站点连接

公司 A 需要和一些商业伙伴进行关键业务合作，这就需要对这些流量进行保护，由于 IPSec VPN 天生具有的特性，使得站点到站点的 IPSec VPN 是最简便且最省钱的办法。

外联网站点到站点 IPSec VPN 的配置仍然包含 ISAKMP/IKE 阶段 1 的配置和 ISAKMP/IKE 阶段 2 的 L2L 会话的配置。

上海分公司有两个 VPN 的配置实例，它们可以共用相同的协商阶段 1 策略，但是采用不同的预共享密钥来增强安全性。

对于阶段2的L2L会话方面，定义需要被保护的流量，定义流量是如何被保护的，定义流量应该转发给谁。这些配置的具体内容将是不相同的。

2. 路由器安全特性配置

在上海分公司连接Internet的接口F1/1上，可以使用访问控制列表，使外来的流量能够正确地访问服务器区域的服务器。由于服务器要对有商业合作的公司开放，采用公司内部的地址必然有很多局限性，采用NAT对服务器的地址进行转换，使得一些业务能够直接被访问，同时增强了公司内部服务器的安全性能。

还可以对需要保证的流量配置QoS，进一步提高性能。

上面这些方法按照工程的实际需要实施，利于公司没有在ISP购买QoS服务，那么配置QoS的作用也就没有体现；如果访问控制列表的一个微小错误，可能导致业务系统的不可用。这些配置本案例中不再举例。

仅仅通过这些网络设备来增强网络的安全性和可靠性，还是远远不够的。比如再增加AAA认证服务器，来对服务器进行认证授权记账；使用专用的流量监控设备；使用防火墙等手段来确保关键业务的正常运作。

8.2.3 该案例实施

1. 上海分公司部分配置

根据上海分公司的具体情况，配置清单如下（不含内联网VPN配置）：

```
ShangHai#configure terminal
ShangHai(config)#crypto isakmp policy 1
ShangHai(config-isakmp)#encr 3des
ShangHai(config-isakmp)#hash md5
ShangHai(config-isakmp)#authentication pre-share
ShangHai(config-isakmp)#group 2
ShangHai(config)#crypto isakmp key cisco456 address 10.3.3.2 no-xauth
!阶段 1 配置结束
ShangHai(config)#crypto ipsec transform-set ShangHaiCo esp-3des esp-md5-hmac
ShangHai(config)#crypto map ShangHai_MAPCo 2 ipsec-isakmp
ShangHai(config-crypto-m)#set peer 10.3.3.2
ShangHai(config-crypto-m)#set transform-set ShangHaiCo
ShangHai(config-crypto-m)#match address mirroredCo
ShangHai(config)#ip access-list extended mirroredCo
ShangHai(config-ext-nacl)#permit ip host 10.2.4.1 host 192.168.1.1
!阶段 2 配置结束
ShangHai(config)#interface FastEthernet1/1
ShangHai(config-if) #ip address 10.2.3.2 255.255.255.252
ShangHai(config-if) #crypto map ShangHai_MAPCo
!在接口激活配置
```

```
ShangHai(config)#ip nat inside source static 172.22.90.1 10.2.4.1
ShangHai(config)#interface FastEthernet1/1
ShangHai(config-if)#ip nat outside
ShangHai(config)#interface FastEthernet1/2
ShangHai(config-if)#ip nat inside
!NAT 配置
ShangHai(config)#router bgp 10
ShangHai(config-router)#network 10.2.3.0 mask 255.255.255.0
ShangHai(config-router)#network 10.2.4.0 mask 255.255.255.0
!路由配置
```

2. 合作公司部分配置

合作公司的配置如下：

```
Partner# configure terminal
Partner(config)#crypto isakmp policy 1
Partner(config-isakmp)#encr 3des
Partner(config-isakmp)#hash md5
Partner(config-isakmp)#authentication pre-share
Partner(config-isakmp)#group 2
Partner(config)#crypto isakmp key cisco456 address 10.2.3.2 no-xauth
!阶段 1 配置结束
Partner(config)#crypto ipsec transform-set Partner esp-3des esp-md5-hmac
Partner(config)#crypto map Partner_MAP 2 ipsec-isakmp
Partner(config-crypto-m)#set peer 10.2.3.2
Partner(config-crypto-m)#set transform-set Partner
Partner(config-crypto-m)#match address mirrored
Partner(config)#ip access-list extended mirrored
Partner(config-ext-nacl)#permit ip host 192.168.1.1 host 10.2.4.1
!阶段 2 配置结束
Partner(config)#interface FastEthernet1/1
Partner(config-if)#ip address 10.3.3.2 255.255.255.252
Partner(config-if)#crypto map Partner_MAP
!在接口激活配置
Partner(config)#router bgp 10
Partner(config-router)#network 10.3.3.0 mask 255.255.255.0
Partner(config-router)#network 192.168.1.0 mask 255.255.255.0
!路由配置
```

对一般的公司合作业务，用户可为每个商业伙伴建立一个 VPN 通道，这使得整个网络的逻辑结构清晰可见，易于管理，对商业伙伴授权也便于审计管理。

在站点到站点的外联网 VPN 中，也需要考虑一些其他问题，比如需要访问一个服务器群，如果对每个服务器都建立一个 VPN 通道，会比较麻烦。这就需要在网络建设之初

对这些服务器群进行一些规划，在定义需要被保护流量时就能简洁一些。还有一个问题，由于公司和商业合作伙伴建立网络之初是没有统一规划的，就会导致地址重叠的问题，这就需要使用NAT技术来解决。

8.3 远程接入VPN

远程访问VPN，通常指一台单用户设备访问VPN网管。例如，一台移动PC或者一个SOHO办公室的一个客户端与VPN网管设备之间的连接应用。

IPSec VPN、PPTP或L2TP VPN，这3种VPN都提供了网络层的保护，其中IPSec远程访问VPN使用较为广泛，在思科产品中称为Easy VPN。和其他两种VPN一样，Easy VPN也包含服务器端和客户端，它们都需要特殊的软件安装在客户端设备上，甚至要培训用户如何去使用它们。

一些公司想要一种比上述提到的3种方案使用起来更简单，维护起来更容易的解决方案。安全套接字层(SSL)开始作为一种协议来保护终端用户设备和Web服务器之间的Web(HTTP)流量。许多厂商看到商机，决定提高SSL的能力，并且使用SSL来实施VPN的解决方案。与前三种VPN相比，SSL VPN最大的一个优点就是不需要在客户端安装VPN软件，用户使用系统已安装的Web浏览器，就可以安全地访问中心站点。

SSL VPN在思科的产品中叫做Web VPN，本章将以思科的Web VPN为例介绍SSL VPN。Easy VPN在此不作介绍，请参看思科的相关文档。

8.3.1 某学校VPN部署整体框架

1. 某学校VPN部署案例背景介绍

随着学校的不断发展，不少教师需要在不同校区办公，要访问到校内资源；不少教师出国或出差，也需要访问校内服务；师生在家做论文，想访问校内图书馆资源等。这些突出的矛盾，给学校网络管理带来很大的问题。每一个重要的特殊的不可拒绝的用户，网络管理员需要在防火墙上打开一个通道，这不仅仅会带来网络管理的难度，也带来不少安全性问题。

因此，通过VPN方式访问校内资源，已经成为一个紧迫的问题。

2. 案例需求分析

按照某学校的情况，现有师生3万余人，需要硬件支持的最大并发用户数应大于或等于3000。但是，就目前业务而言，并发用户数达到100就能满足需求，在未来用户需要时，可以通过购买授权的方式扩充并发用户数，而不必更换硬件。为使得设备具有扩展性，需要支持RADIUS、LDAP等多种认证方式，对接入用户实现认证。使用SSL VPN方式接入时，用户可以以与校内用户同样的身份访问校内所有网页资源和数字图书馆资源。该方式支持用户直接通过浏览器安装VPN客户端插件访问校内CS模式的资源，包

括使用 Telnet、SMTP、POP3、FTP 和 SIP 协议的校内应用。需要设备本身提供日志功能,日志可以以 syslog 方式导出到日志服务器上。日志内容应包含 VPN 用户登录、登出的日期和时间。当设备出现故障时,不影响园网本身的连通性,部署该设备不能影响现有校园网数据的传输。

对某学校现有出口网络结构进行简化,形成了如图 8-4 所示的某学校出口简图。该学校的出口其实非常复杂,出口路由器连接了多个 ISP,下一步还打算连接新联通的链路、教育信息网等链路。对外多条链路的选择是通过一个专门的链路负载均衡设备来实现。核心设备带有防火墙功能,是一个典型的大型园区网络结构。

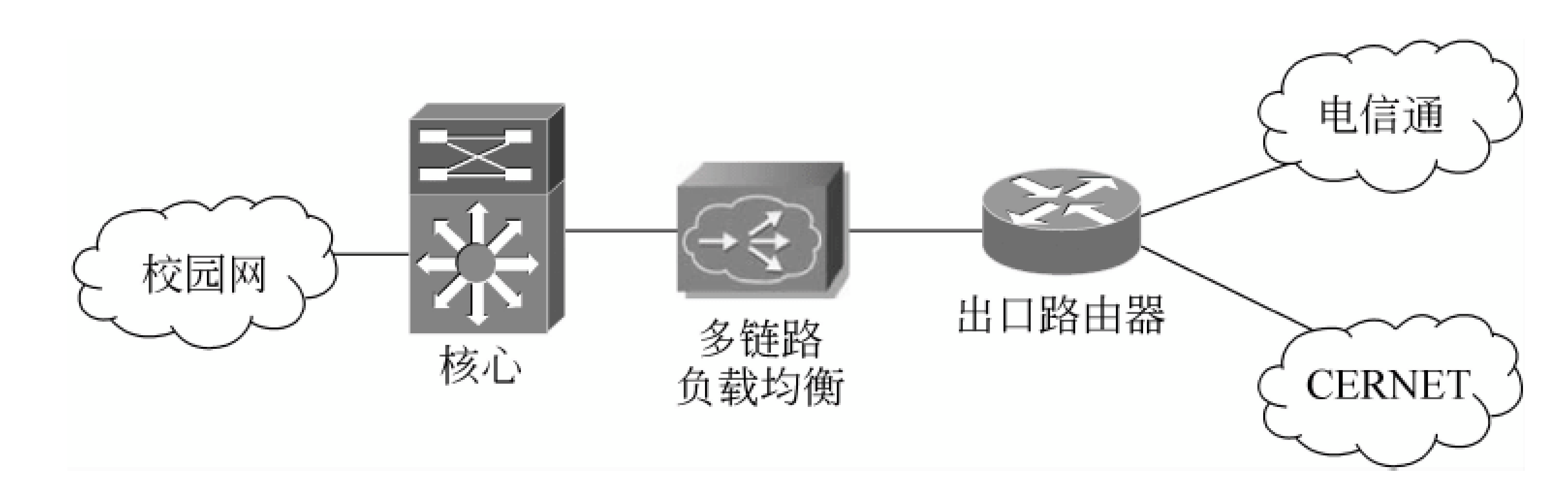


图 8-4 某学校出口简图

3. 技术方案确定

根据需求,这是一个 SSL VPN 的应用,可选的设备很多,各大网络厂商都能支持 SSL VPN,如思科的 ASA、具有安全特性的 IOS 路由器等。本案例中,出口路由器 IOS 可以支持 SSL VPN,但是出于安全考虑,它不能作为远程接入 VPN 的服务器端。

技术路线:根据需求,使用 SSL VPN 技术。

设备选择:Array Network(在 Frost & Sullivan 的 2007 年—2009 年调查报告中,Array Network 公司的 SSL VPN 产品在中国大陆销售排名第一)的 SPX 4800 产品满足需求,也是该校实际使用的产品。但是本文以思科的产品为例配置,故选择了 ASA 5550 这款产品(如果只是用来做 WebVPN,就是大材小用了)不仅仅用来做 WebVPN,还可以分担目前防火墙的一些工作,但是这个案例中不对防火墙功能进行讨论。

地址规划:经过简化,考虑到和内部用户地址(使用了 RFC 1918 中的 B 段私有地址)的一致性,SSL VPN 用户采用 172.31.0.0/18 这段地址。实施 SSL VPN 后的网络结构如图 8-5 所示。

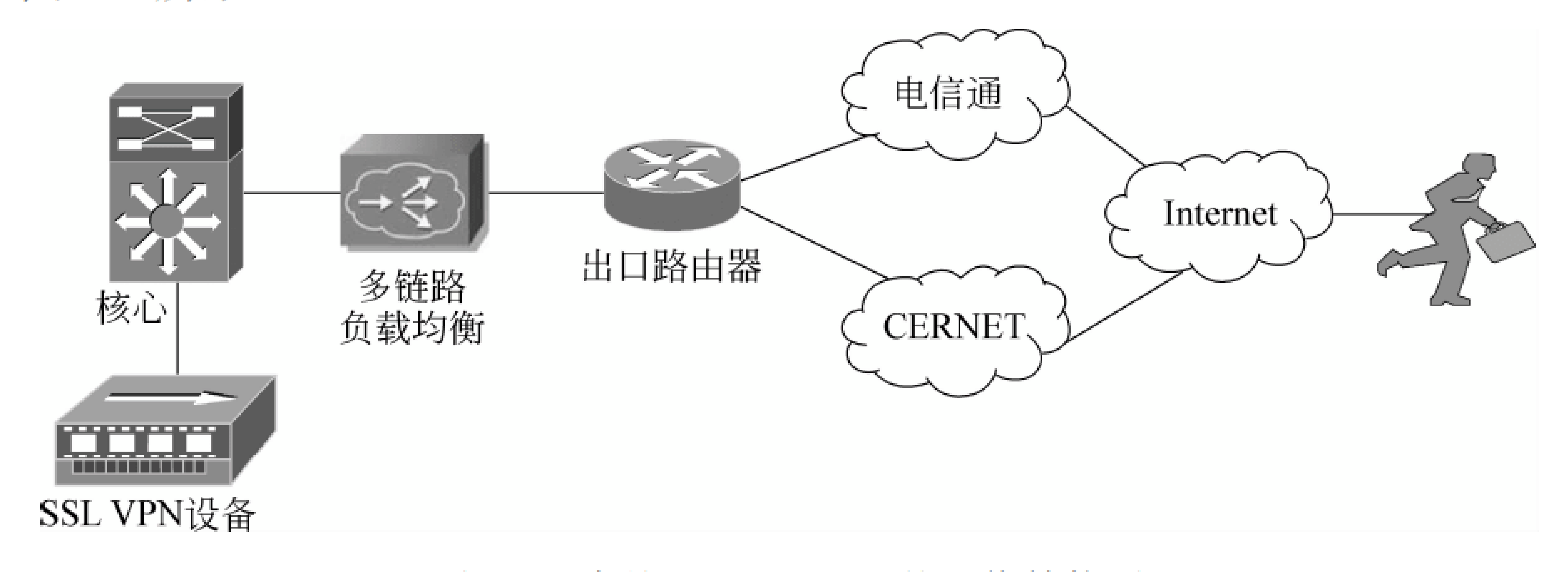


图 8-5 实施 SSL VPN 后的网络结构图

8.3.2 WebVPN 远程访问连接

WebVPN 是远程访问连接的一个方式，现在流行的浏览器(具体支持的浏览器，参看设备相关手册)都能够很好地支持。对于 WebVPN 的配置，大概包含以下 4 个步骤。

第 1 步，在配置 WebVPN 之前，需要配置上述内容，这是必须配置的。具体包含建立 AAA 来验证 WebVPN 的用户；建立 DNS 来解析 URL 的名字信息；配置 HTTPS 所需要的证书(ASA 设备为可选，路由器必须配置)。

第 2 步，在上述必备条件具备后，进行 WebVPN 的配置。

第 3 步，在主页上建立 URL 和端口转发条目。

第 4 步，维护监控和故障诊断与排除 WebVPN 的连接。

1. 必须配置的内容

(1) AAA 的配置。当用户访问 WebVPN 时，用户名密码必须进行验证。用户名和密码可以存储在 ASA 本地，或者定义在使用 TACACS+ 或者 RADIUS 安全协议的一台 AAA 服务器上。

当利用本地来作认证，使用的基本命令如下：

```
ciscoasa(config)#aaa local authentication attempts max-fail 3
```

如果利用非本地的数据来作认证，使用下面的基本命令：

```
ciscoasa(config)#aaa-server server-tag[(interface-name)]host{server-ip|name}
[key][timeout seconds]
ciscoasa(config)#aaa-server server-tag protocol server-protocol
ciscoasa(config-aaa-server-group)#max-failed-attempts 3
```

首先指定 AAA 服务器的地址，以及 ASA 与 AAA 服务器之间认证的 key；然后需要指定所用的认证协议(如 RADIUS、TACACS+ 等)；最后可以指定用户最大的尝试次数，默认即为 3 次。AAA 服务器可以用思科公司的 ACS 来实现，而且思科的解决方案中也往往使用了 ACS。有关 TACACS+ 或者 RADIUS 协议，请参考前面的介绍。

注：ACS 是思科的一个软件，专门用来提供 AAA 服务。ACS 软件的使用非常广泛，如对所有思科网络设备进行认证、授权、记账。还能与思科的语音、无线设备进行配合，提供一个思科的整体解决方案。思科网站提供了 ACS 的很多文档，非常有用。

(2) DNS 相关配置。DNS 有两个作用：为了保护 SSL 的链接，产生一个 RSA 密钥对时需要域名；为了解析 URL 中的名字，也需要 DNS 配合。

配置一个 DNS 组，可以指定多个 DNS 服务器地址。用户需要配置如下命令：

```
ciscoasa(config)#hostname name
ciscoasa(config)#dns server-group name
ciscoasa(config-dns-server-group)#domain-name name
ciscoasa(config-dns-server-group)#name-server ip_address[ip_address2][...][ip_
```

```
address6]
```

为了产生用于 SSL 证书的 RSA 密钥，必须在 ASA 上有 domain-name，但 ASA 其实有一个默认的域名，路由器上却没有。ASA 默认的主机名为 ciscoasa，而 name-server 是用来指定 DNS 服务器，解析 FQDN 全域名（FQDN，Fully Qualified Domain Name）的。

（3）SSL 证书配置。获取证书有两种方法，从 CA 获取一个证书，或者建立一个自签发的证书。而在一般企业中，使用外部的 CA 基本没有必要，在 ASA 上面建立一个自签发的证书就可以满足要求。ASA 默认 SSL 是开启的，可以不用配置。如果要使用其他的自签发书，方法和在路由器上一样。ASA 的基本命令如下：

```
ciscoasa(config)#crypto ca trustpoint Trustpoint Name
ciscoasa(config-ca-trustpoint)#enrollment self
ciscoasa(config-ca-trustpoint)#subject-name X.500 name
ciscoasa(config-ca-trustpoint)#keypair name
ciscoasa(config)#ssl trust-point{trustpoint[interface]}
ciscoasa(config)#crypto ca enroll trustpoint[noconfirm]
```

2. 配置启用 WebVPN

启用 WebVPN 非常简单，需要在具体的接口下启用 WebVPN，命令如下：

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable ifname
```

通过 webvpn 命令进入 webvpn 配置模式，然后在某一接口上启用 webvpn。

注意： *启用 webvpn 之前，一定要在接口模式下用 ifname 命令，为该接口配置一个名字。*

3. 在主页上建立 URL 等工作

ASA 对这方面的配置已经实现图形化操作，不少命令不再被支持，这和路由器的配置不太一样。

4. 维护监控和故障诊断与排除 WebVPN 的连接

WebVPN 启用后，可以使用 show 命令，对 WebVPN 的连接情况进行查看，主要有以下命令：

```
ciscoasa#show vpn-sessiondb
ciscoasa#show webvpn statistics
```

使用 show ssl 命令，可以查看当前 SSL 的一些基本配置，比如数据传输使用的加密协议、SSL 连接使用的版本等。

8.3.3 该案例的实施

虽然前面的命令配置内容不多，但是看起来也还是很复杂。思科公司推出 ASDM 图形化界面，对 ASA 进行配置，使防火墙的配置更加简单。下面将用图形化界面对 WebVPN 进行配置。

1. 实施前的准备工作

首先需要在 ASA 上配置一些基本命令，使 ASDM 能够正常访问。确认 ASA 的系统版本以及 ASDM 的版本，本案例中使用的是 asa804-k8.bin、asdm-621.bin。

确认版本后，先要配置管理接口 IP，本案例取名为 management。然后输入如下命令：

```
ciscoasa(config)#http server enable
ciscoasa(config)#http 0.0.0.0 0.0.0.0 management
```

此时，就可以通过 Internet Explorer 浏览器访问管理接口的 IP 地址，出现 ASDM 安装提示，如图 8-6 所示(注意需要安装 Java 的运行环境)。安装并启动 ASDM 软件，输入 ASA 管理接口的 IP 地址，单击 OK 按钮。

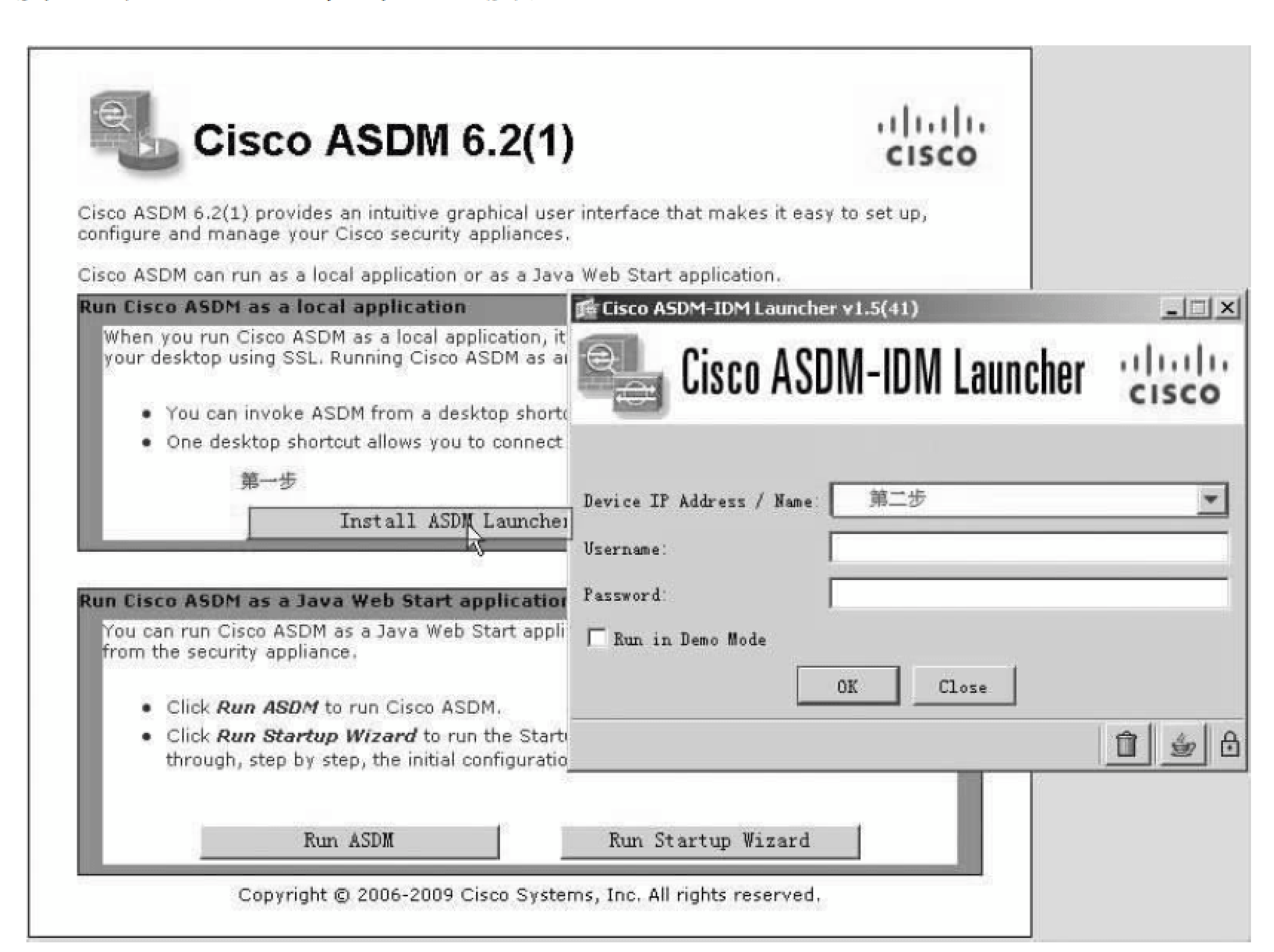


图 8-6 ASDM 软件

2. 必需的基本配置

启动 ASDM 后，进入 ASA 的配置界面，如图 8-7 所示。单击 Configuration 选项卡，然后找到左侧的 Device Setup 栏，选择 Interface，编辑要配置的接口，进行配置。

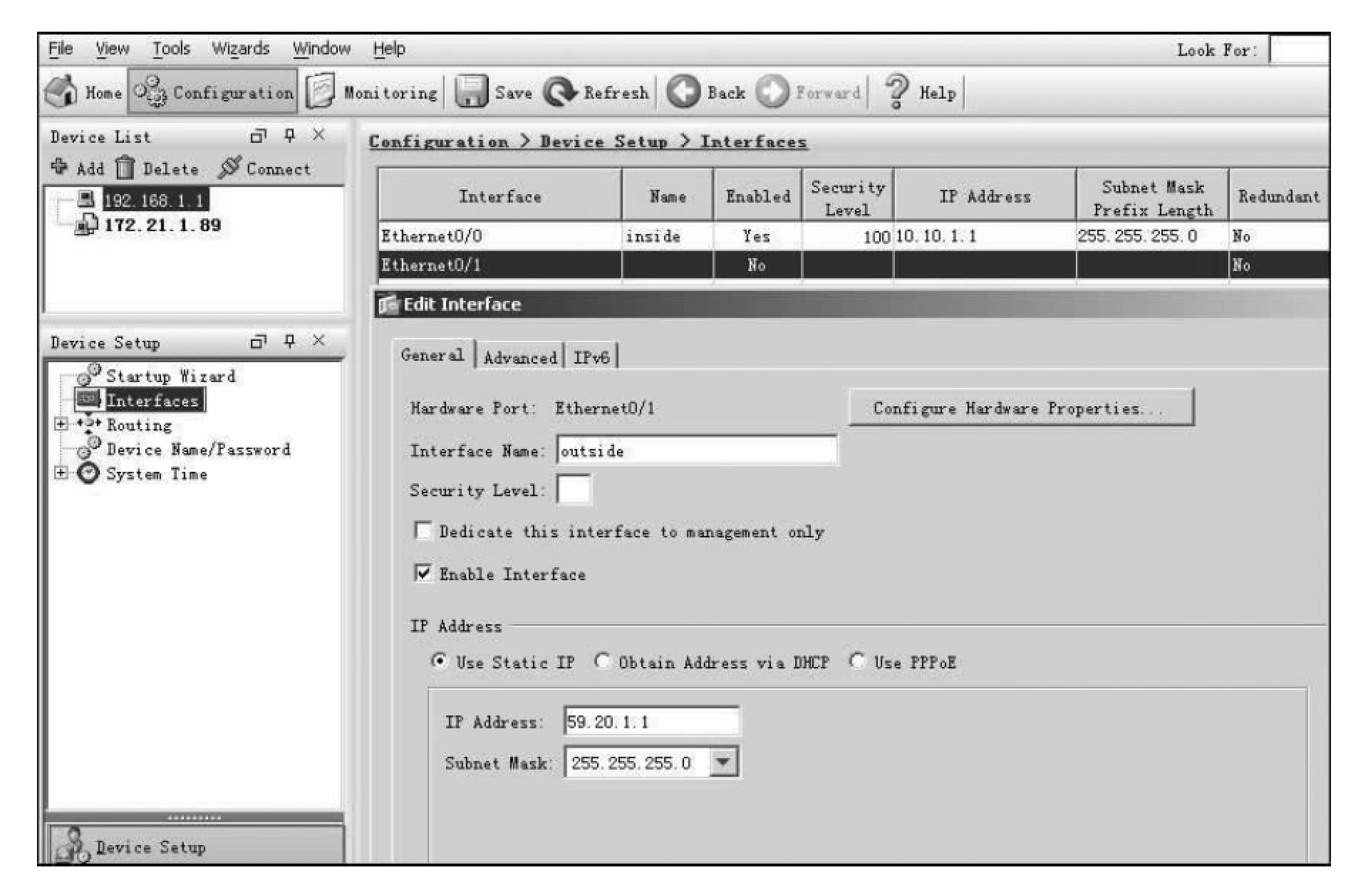


图 8-7 ASA 的配置界面

注意：*要启用接口。*

配置好接口后，需要检查 ASA 的路由配置是否正确，本案例中配置了静态路由，如图 8-8 所示。

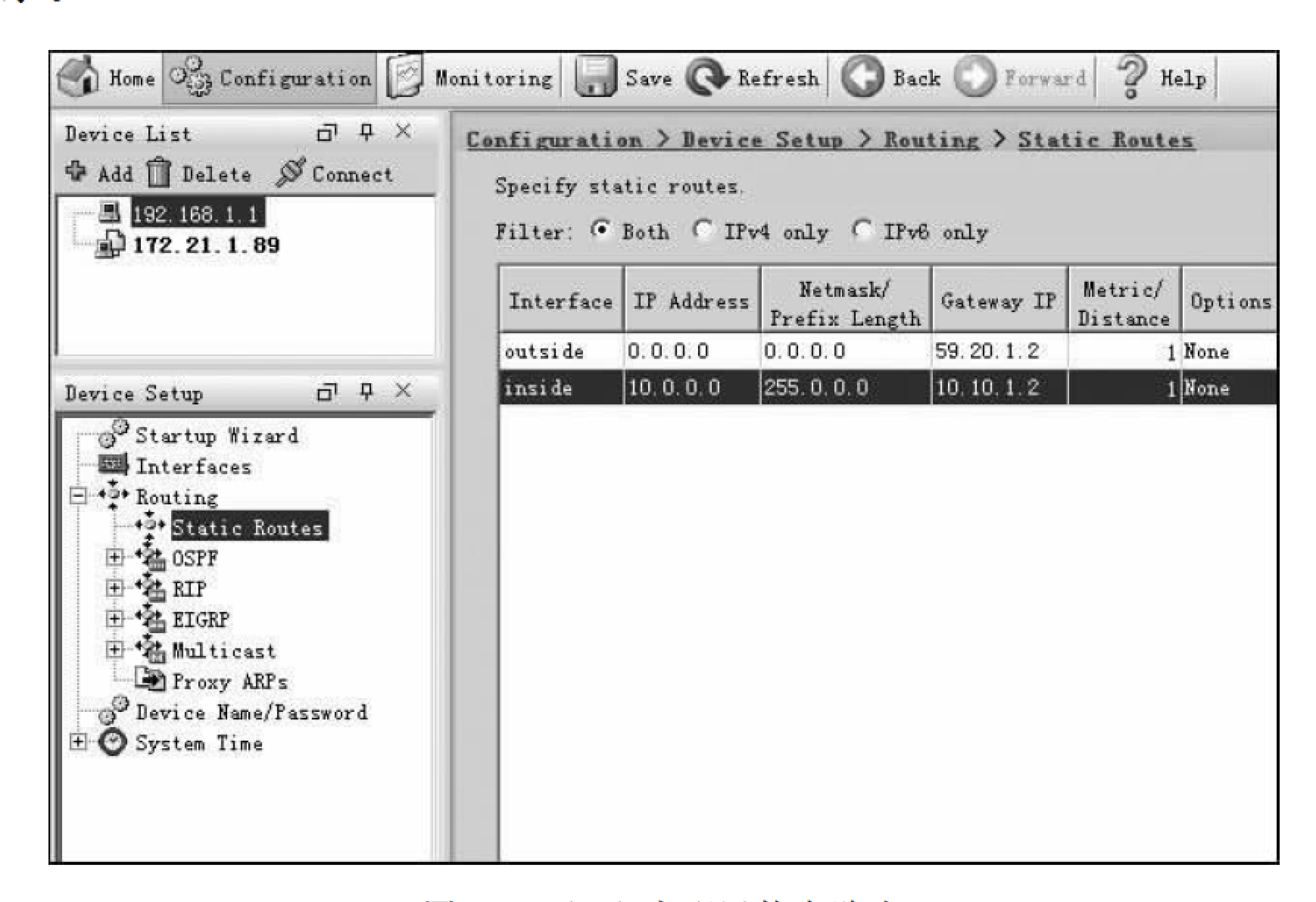


图 8-8 ASA 中配置静态路由

选择 Device Name/Password 项，配置 ASA 名以及域名，如图 8-9 所示。若不进行配置，将使用 ASA 默认配置。记住，还需要配置 DNS，本例不再介绍。

然后进行 AAA 的配置，如图 8-10 所示。本案例实际使用的是外带 ACS，但是由于本文着重讨论 VPN，在此使用本地账户。对于本地账户，可以在 VPN Policy 对用户的一

些其他特性进行配置，默认是继承了所有的特性。

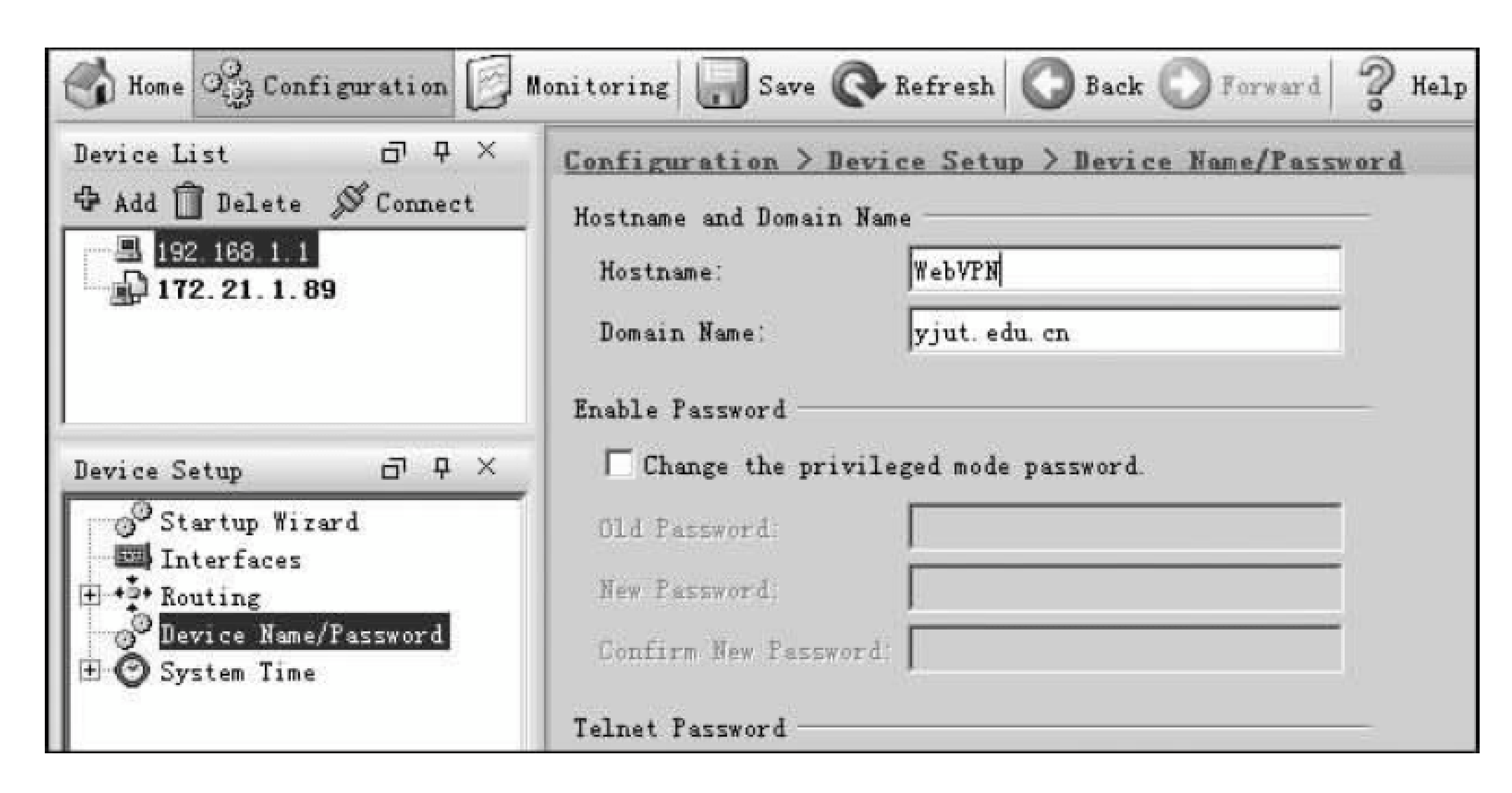


图 8-9　ASA 中配置域名

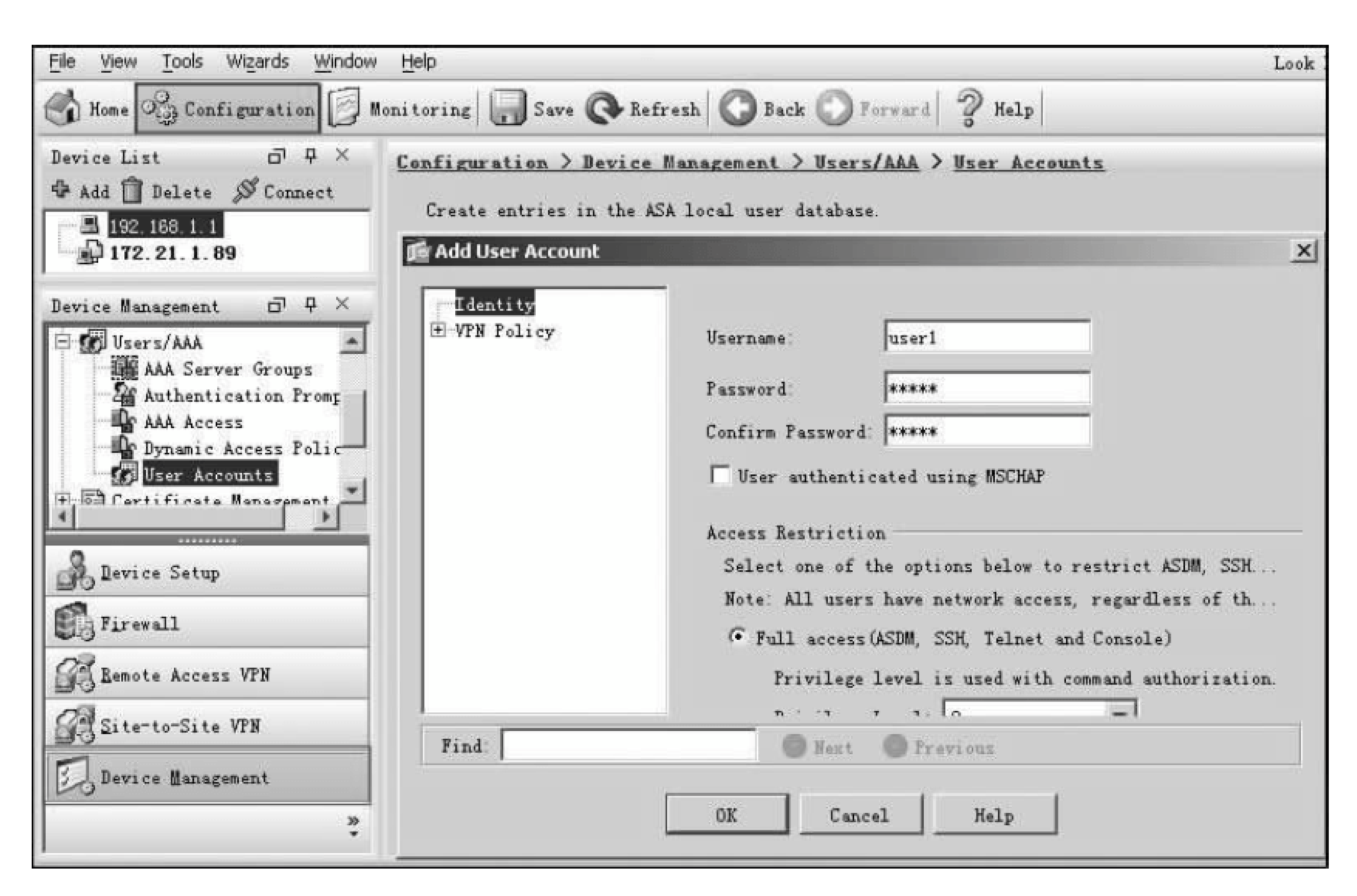


图 8-10　AAA 配置

必需的配置基本完毕，还剩下 SSL 证书的配置。之前说过，SSL 的配置可采用默认配置，但是为了保证安全性，本例将建立一个自签发的证书，而不采用默认的证书，证书配置如图 8-11 所示。

至此，基本配置已经完成。添加证书后，还需要在 SSL 中使用才起作用。本例使用如下命令手动进行，当然也可以通过图形化界面来配置。

```
WebVPN(config)#ssl trust-point SSLVPN
```

3. 启用 WebVPN

启用 WebVPN 的命令非常简单，本案例使用的是 clientless 的 SSL VPN。如图 8-12 所示，勾选 outside 接口的选框，即在 outside 启用了 WebVPN。

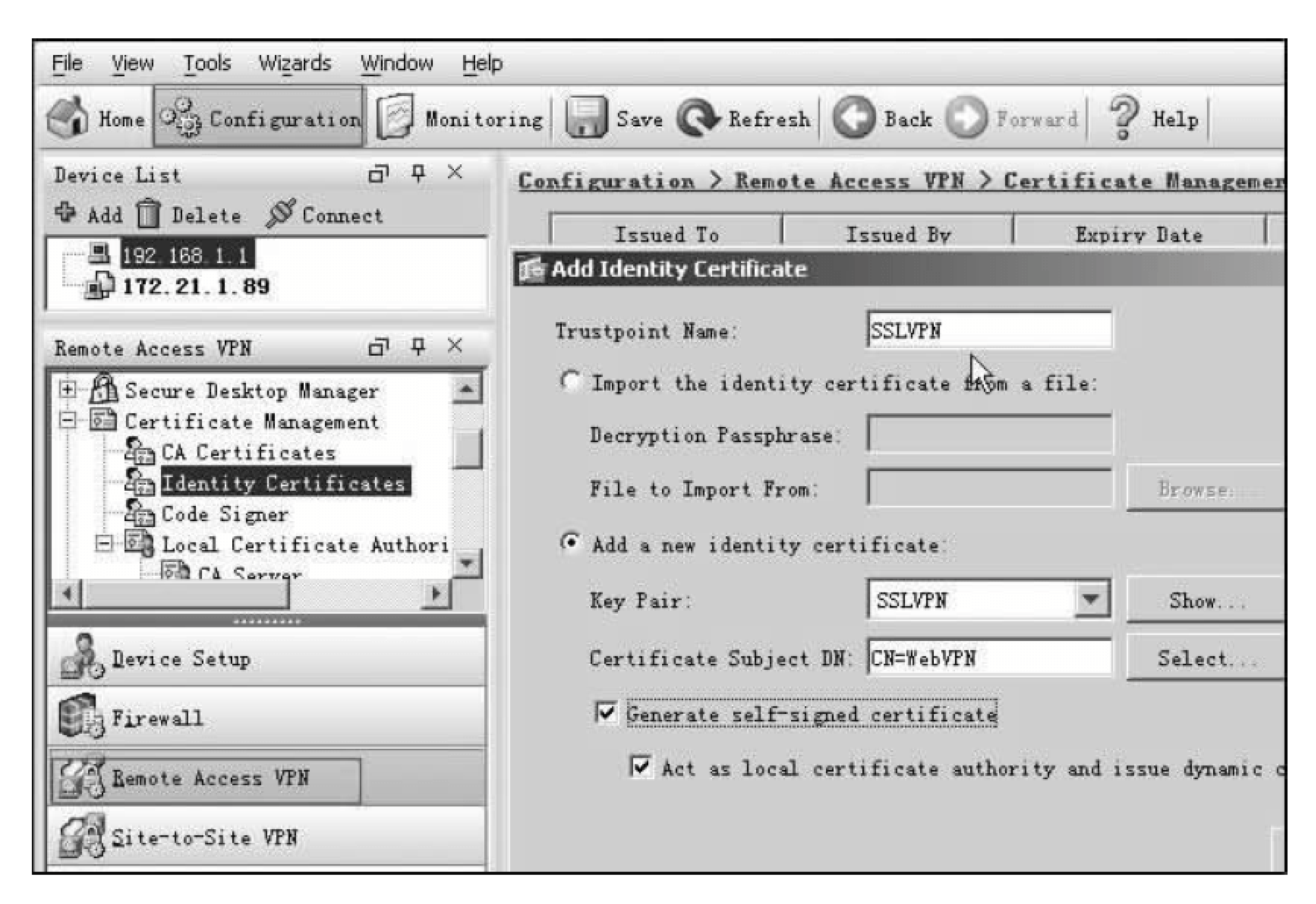


图 8-11　SSL 证书配置

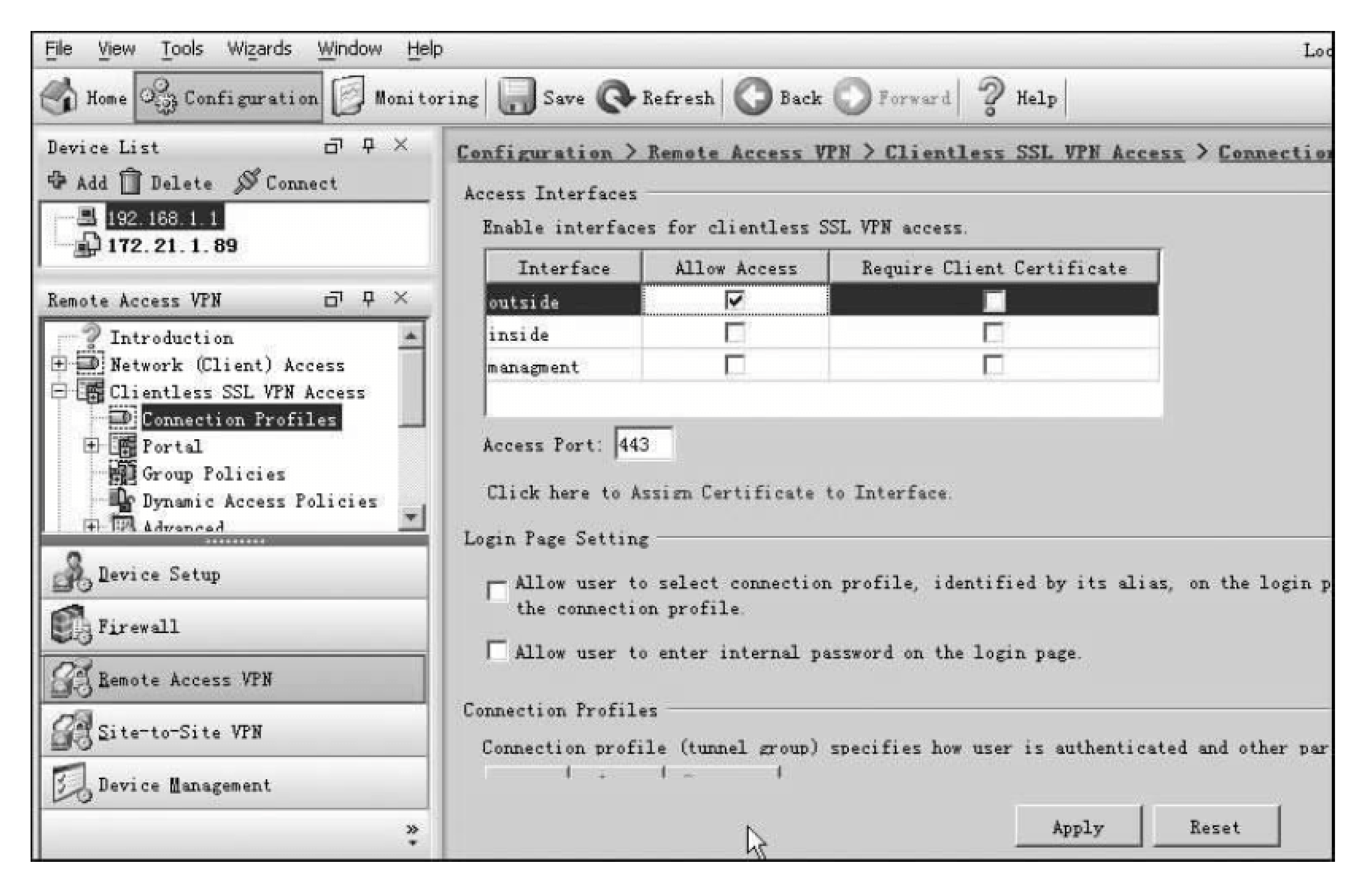


图 8-12　WebVPN 的配置

经过以上配置，WebVPN 就能正常工作了。当然，基本配置完成后，我们也可以在菜单 Wizards 中选择 SSL VPN Wizards，一步一步地启用 WebVPN。

4. 其他工作

以上配置完成后，只能完成一些基本的 WebVPN 操作，如访问网站、使用 FTP 等。还有很多其他工作要做，如对加密算法的配置、对 Portal 的配置等。本案例着重介绍思科的 Smart Tunnel 功能，如图 8-13 所示，用来解决 WebVPN 使用的一些问题，如一些常用 Telnet 加密访问服务器，使用 Windows 自带软件登录远程桌面等。

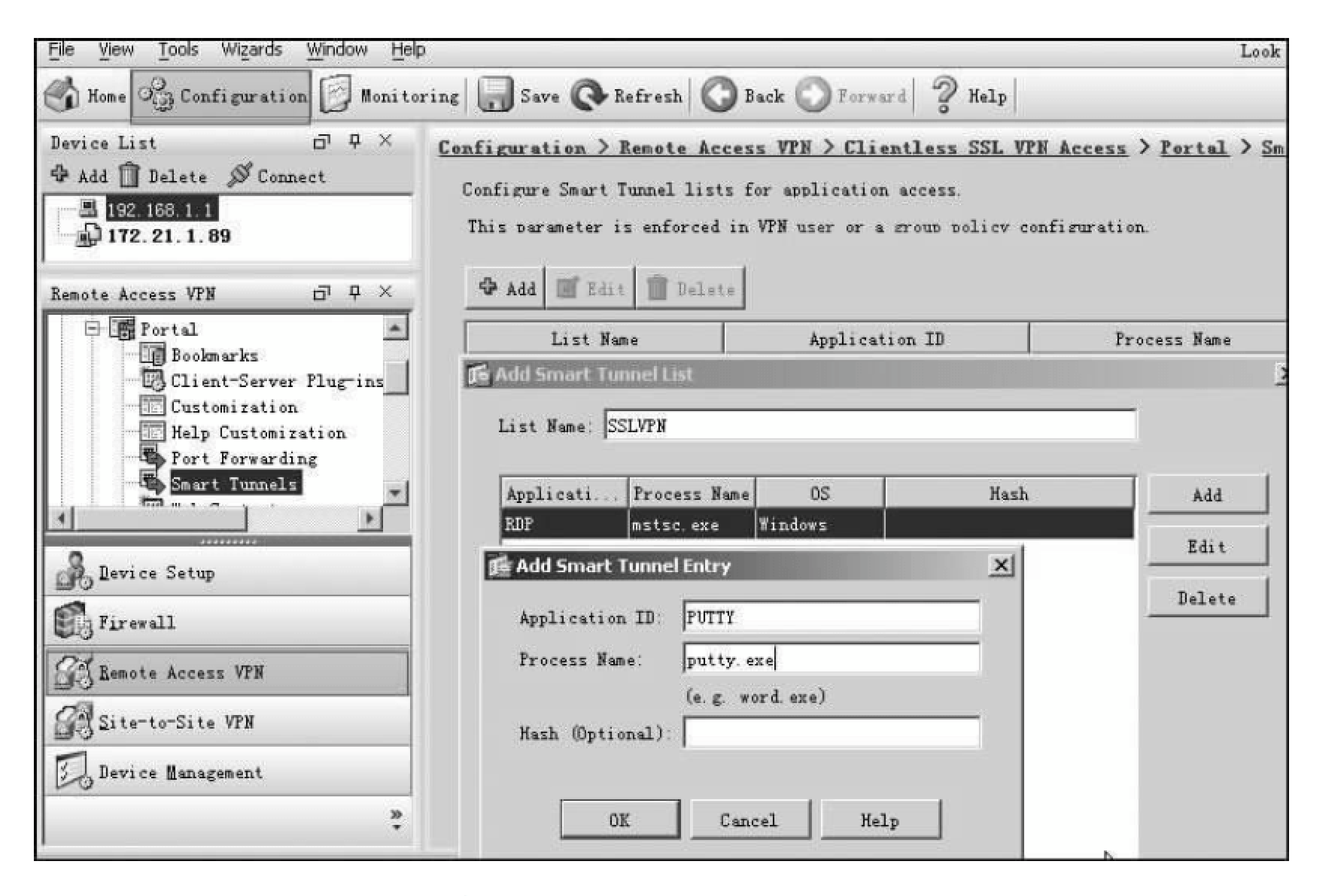


图 8-13 Smart Tunnel 配置

建立好列表后，在 connection profiles 中，选择所使用的 WebVPN 的 connection profile 策略，如图 8-14 所示，进行编辑，在 Basic 选项卡中管理所使用的组策略。对于组策略进行编辑，选择 portal 选项卡，找到 Smart Tunnel，选择之前制定的 Smart Tunnel List，并勾选自动启动选项。对于选择的 Smart Tunnel List，也可以再次进行管理，如图 8-15 所示。

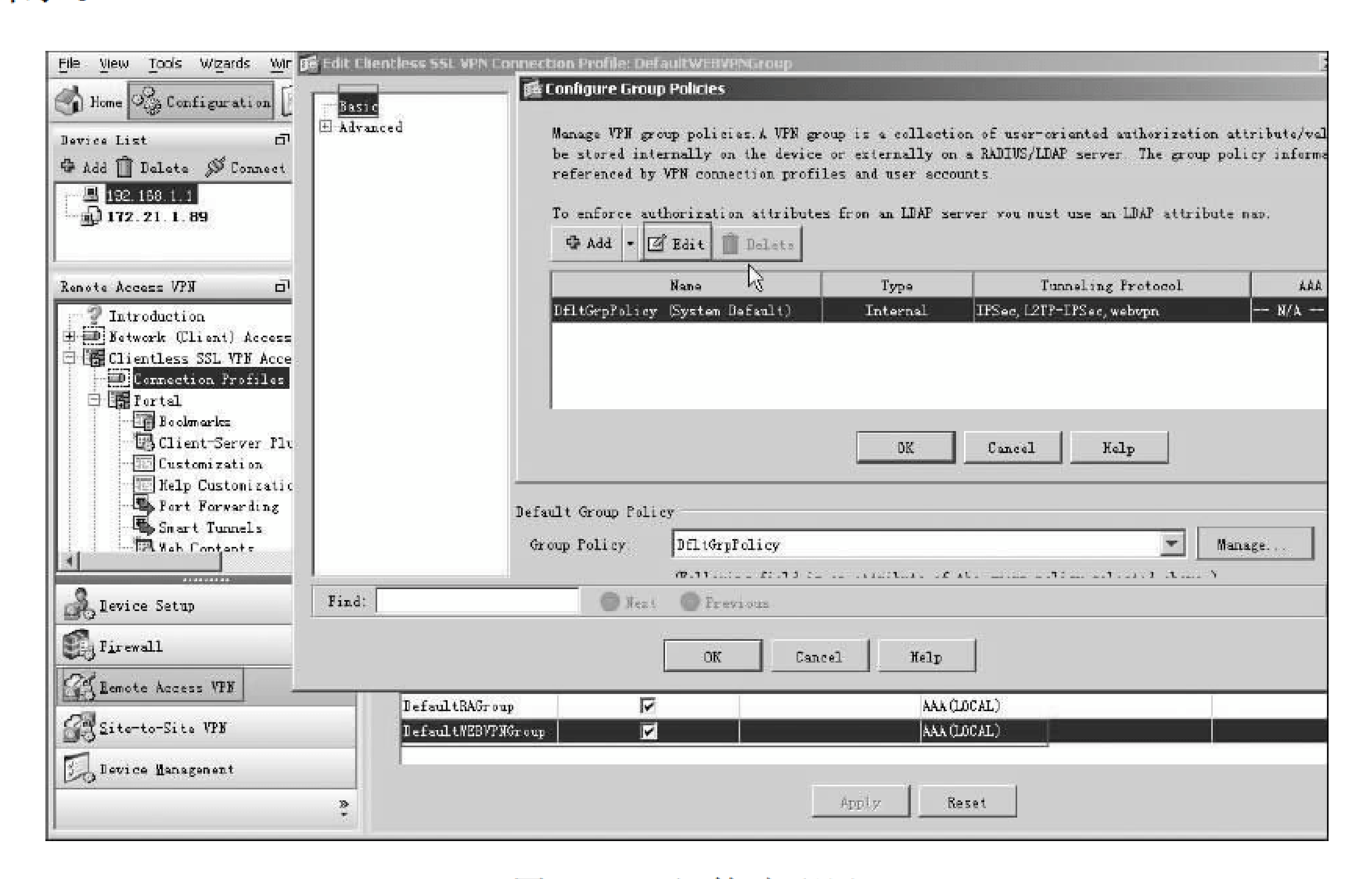


图 8-14 组策略配置

5. 维护与监控 WebVPN

WebVPN 配置完成后，可以通过一些基本命令来检查是否正常运行，或排除错误。如发现用户的证书并不是新建的，可以通过 show ssl 来查看 SSL 的信任点是否更改为我

们需要的。

```
ciscoasa# show ssl
Accept connections using SSLv2,SSLv3 or TLSv1 and negotiate to SSLv3 or TLSv1
Start connections using SSLv3 and negotiate to SSLv3 or TLSv1
Enabled cipher order: 3des- sha1
Disabled ciphers: des- sha1 rc4-md5 rc4- sha1 aes128- sha1 aes256- sha1 null- sha1
SSL trust-points:
    Default: SSLVPN
Certificate authentication is not enabled
```

如果显示为 No SSL trust-points configured,表示没有应用自签发证书。

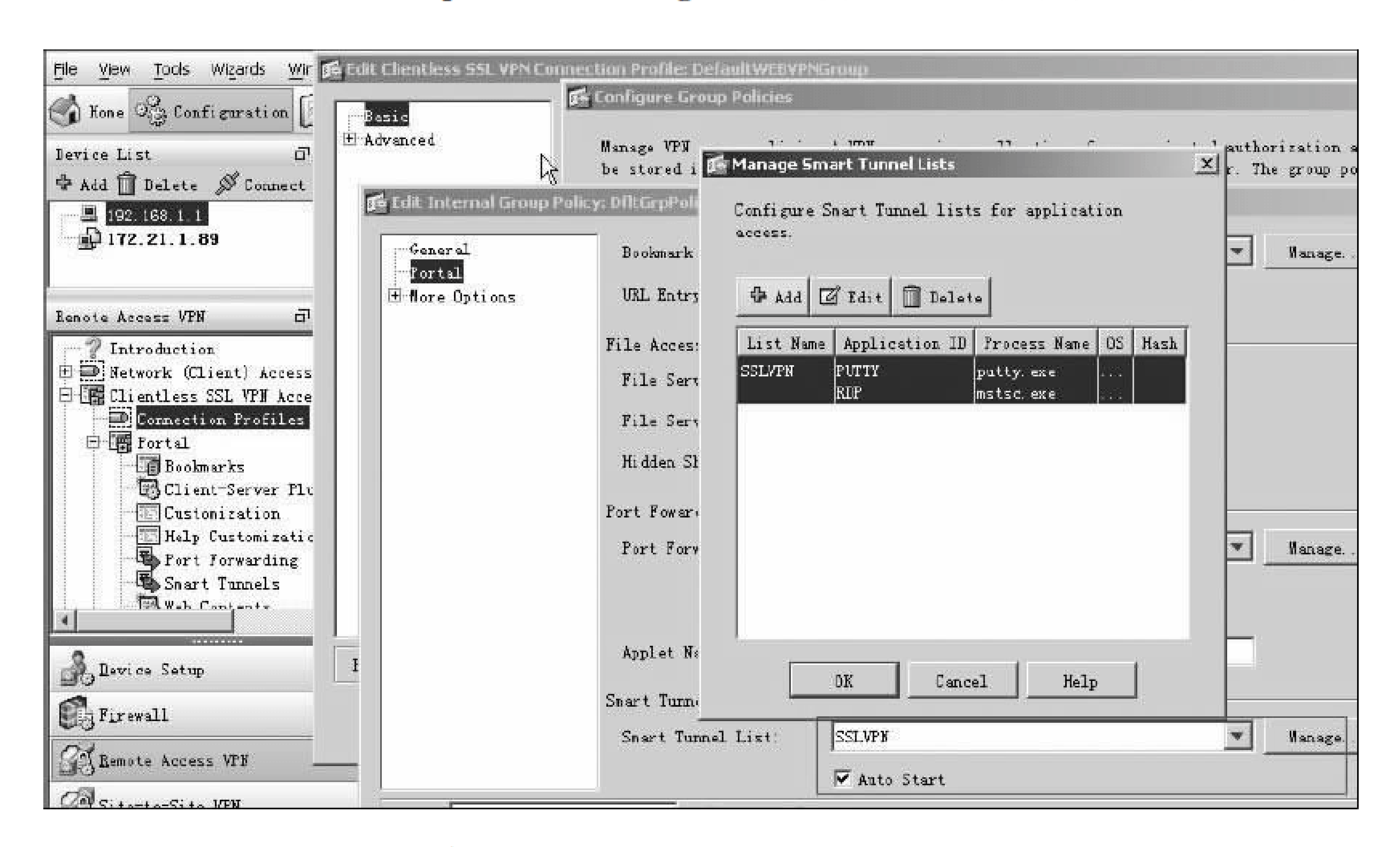


图 8-15 Smart Tunnel List 配置

使用 show webvpn statistics 可以查看一些基本的统计信息。利用 show vpn-sessiondb 来查看登录成功的用户信息,如图 8-16 所示。当然,也可以用 ASDM 来查看。

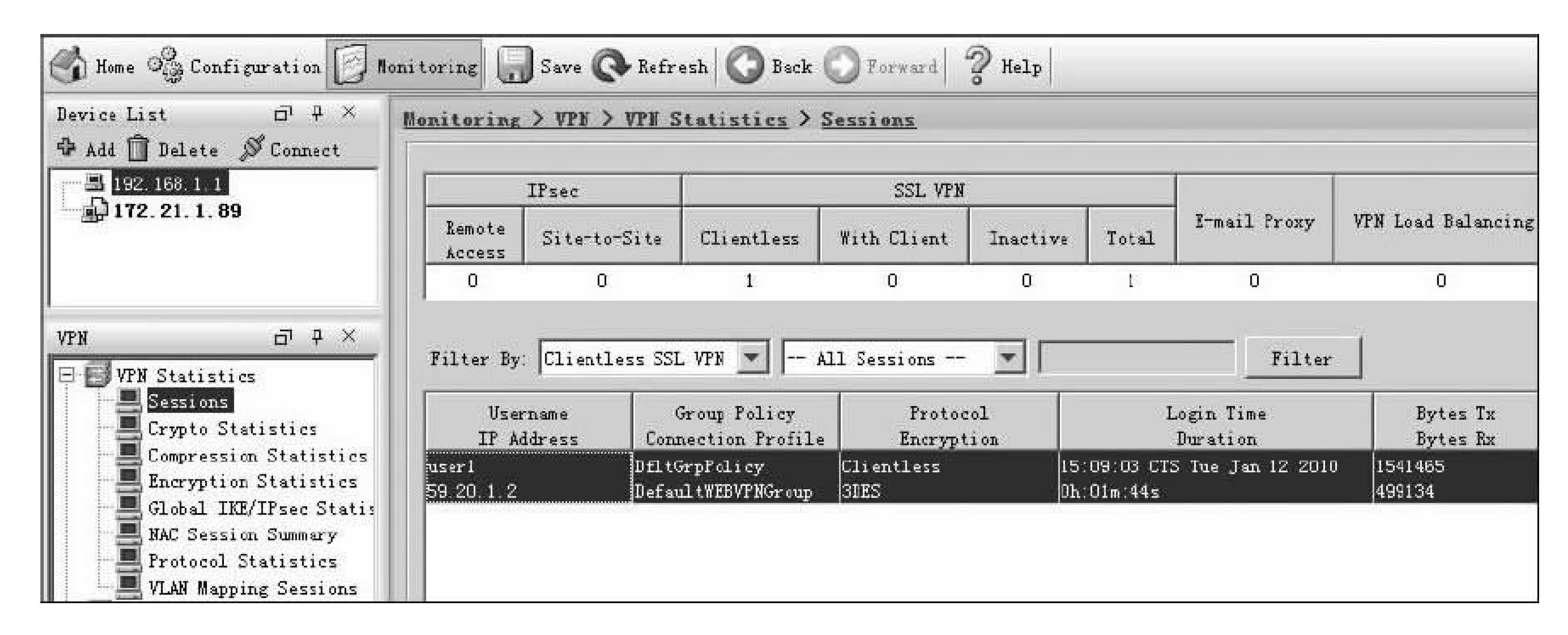


图 8-16 登录成功的用户信息

在使用过程中,有的用户发现 Smart Tunnel 启动不了。请把 WebVPN 的站点加入到信任列表中,在客户端安装控件后,Smart Tunnel 就能启动了。

习题8

1. 公司A自己申请了一段IPv6地址以及一段IPv4地址,通过光纤接入某ISP,该ISP提供IPv4和IPv6服务,实现了IPv4和IPv6的接入。现因业务需要,公司A在外地的分公司B也需要连接IPv6网络,公司B使用ADSL方式连接到IPv4网络,无法通过ISP直接连接到IPv6网络。请读者分析,在上述情况下,如何保证公司A和公司B能安全连接。

解决思路分析:公司B可以与公司A建立IPv6 over IPv4的隧道,来访问IPv6网络。但公司B没有固定的IPv4地址,无法直接建立IPv6 over IPv4的GRE隧道,则需要先为公司B网络分配固定的IPv4地址,可以通过与公司A建立VPN,公司A会向公司B分配固定的IPv4私有地址,通过公司A与公司B的私有地址建立GRE隧道,然后建立IPv6 over IPv4隧道。

2. 假设ISP给公司A和商业合作伙伴的地址非常有限,既要做NAT,又要做站点到站点的VPN,应如何配置此类VPN网络?

3. 利用ASA的ASDM软件配置带客户端的SSL VPN,或使用路由器SDM软件,对第一个案例进行图形化配置。

4. 通过上述案例的学习,自学并配置基于IPSec的Remote Access VPN。

5. 通过厂商的扩展,WebVPN越来越适应现在企业的需要,解决了企业的大多数问题。但如何个性化企业自己的WebVPN站点,如何使站点的使用更加方便呢?请对第8.3.3节的案例进行优化或美化。

第 9 章　VPN 产品介绍和选购标准

根据各行各业的经验累积，对企业信息而言，可以说企业级 VPN 产品应用主要表现为实时信息传递与高安全性两方面，具有很大的优势与价值。

由于企业级 VPN 在互联网上使用加密隧道，在所有分支外点与总部中心端之间建立一个私有且安全的多点互联网络，具有安全、简单、方便、节省成本的特性。通过 VPN 网络，可让企业各分支外点、移动用户达到如同置身在中心端内网的效果，使远程访问 ERP、存取公司内部数据等工作快速、实时又方便。此外，VPN 的另一项特色是具有加密的功能，因此企业的所有信息通过 VPN 网络即可达到安全保密的效果。整体而言，企业需要让各外点远程达到实时同步共享中心端资源，增加企业对外竞争力，同时保证机密数据安全保密。

目前，市面上企业级 VPN 产品有高、中、低三级产品，但几乎都是由 3 个最主要的协议所组成，包含 IPSec、SSL、PPTP 等协议类型。而要找出最适合企业的 VPN 产品，必须对这 3 种主要协议的应用特性有所了解。

一般而言，IPSec 是运用在网关对网关的设备，也就是中心端对规模较大的外点所采用的设备，同时也是目前运用最普及的 VPN 协议。但其设定多达 20 多个步骤，对于不太具备网关知识的企业用户而言，弊端是略显繁复；对网管而言，也是一大门槛。但 IPSec 协议设定一旦联机后，所有信息也跟着开放了，每个人可使用的信息均相同，无法设定不同人可有不同的存取权限，这对于企业只想开放有限的权限给合作伙伴的考虑而言，是一个比较大的瓶颈。

相对 IPSec 而言，SSL 是近年来 VPN 设备市场中异军突起的通信协议。它除了拥有实时分享与信息安全两大基本优势之外，还可针对不同的用户属性设定不同的使用权限。比如，只允许合作伙伴使用 FTP 服务、允许出差在外的业务人员使用 ERP 数据存取、允许分支外点拥有使用全部服务的权限等。只需要用标准浏览器登入中心端应用、存取内网资源，解放外部员工 VPN 联机的地点限制。对于 VPN 产品而言，SSL VPN 的加入更加强化了企业信息安全。但对于某些企业来说，必须考虑相对 IPSec 较高的建置成本，因此，若企业不需要管控人员权限，IPSec 倒是不错的选择。

至于 PPTP，多半运用在信息流量不大、不需要实时信息的小分点机构或移动用户。PPTP 的使用虽然较为简单，但并没有完整的加密机制，所以在企业机密安全考虑上会有比较高的风险存在。因此，在企业各点，包括小分点或移动用户，我们还是建议采用 SSL VPN 或 IPSec VPN 协议，在保证信息安全性上会比较适合。

9.1 国外主流产品

9.1.1 Cisco 公司在 VPN 方面的产品

Cisco 公司在路由交换领域处于业界公认的领先地位。目前，Cisco 公司已经拥有了全套 VPN 设备，能够为各种规模、不同行业的企业制定 VPN 解决方案。在 Cisco 公司硬件 VPN 方案中，主要有集中器、路由器和防火墙这 3 类产品。

1. Cisco ASA 5500 系列下一代防火墙

如图 9-1 所示，思科 ASA 5500 系列自适应安全设备是思科推出的下一代防火墙安全解决方案，它是提供了新一代安全性和 VPN 服务的模块化平台。企业可以根据特定需求订购不同版本，做到逐步购买、按需部署，灵活方便地扩展安全功能。



图 9-1　思科 ASA 5500 系列

为了确保网络安全，以往企业通常购入一系列专用型安全设备，造成投入成本大、部署繁复、管理复杂的局面。推出 Cisco ASA 5500 系列自适应安全设备之后，思科能够以物理设备的方式，在同一个平台上提供融合的多功能安全和 VPN 服务。借助融合型防火墙、入侵防御系统(IPS)和网络 Anti-X 服务，客户可以使用 Cisco ASA 5500 系列部署各种威胁防御和安全服务。对于 VPN 服务，Cisco ASA 5500 系列能够灵活地提供定制的解决方案，满足 SSL VPN 和 IPSec 远程接入以及站点间的连接要求。

由于 Cisco ASA 5500 系列自适应安全设备能够提供多种 VPN 和安全服务，因而能够一机多用。企业可以将其部署为单功能独立设备，也可以作为组合解决方案，应用的体系结构如图 9-2 所示，可以根据特殊部署环境定制 Anti-X、IPS、防火墙和 VPN 应用。在

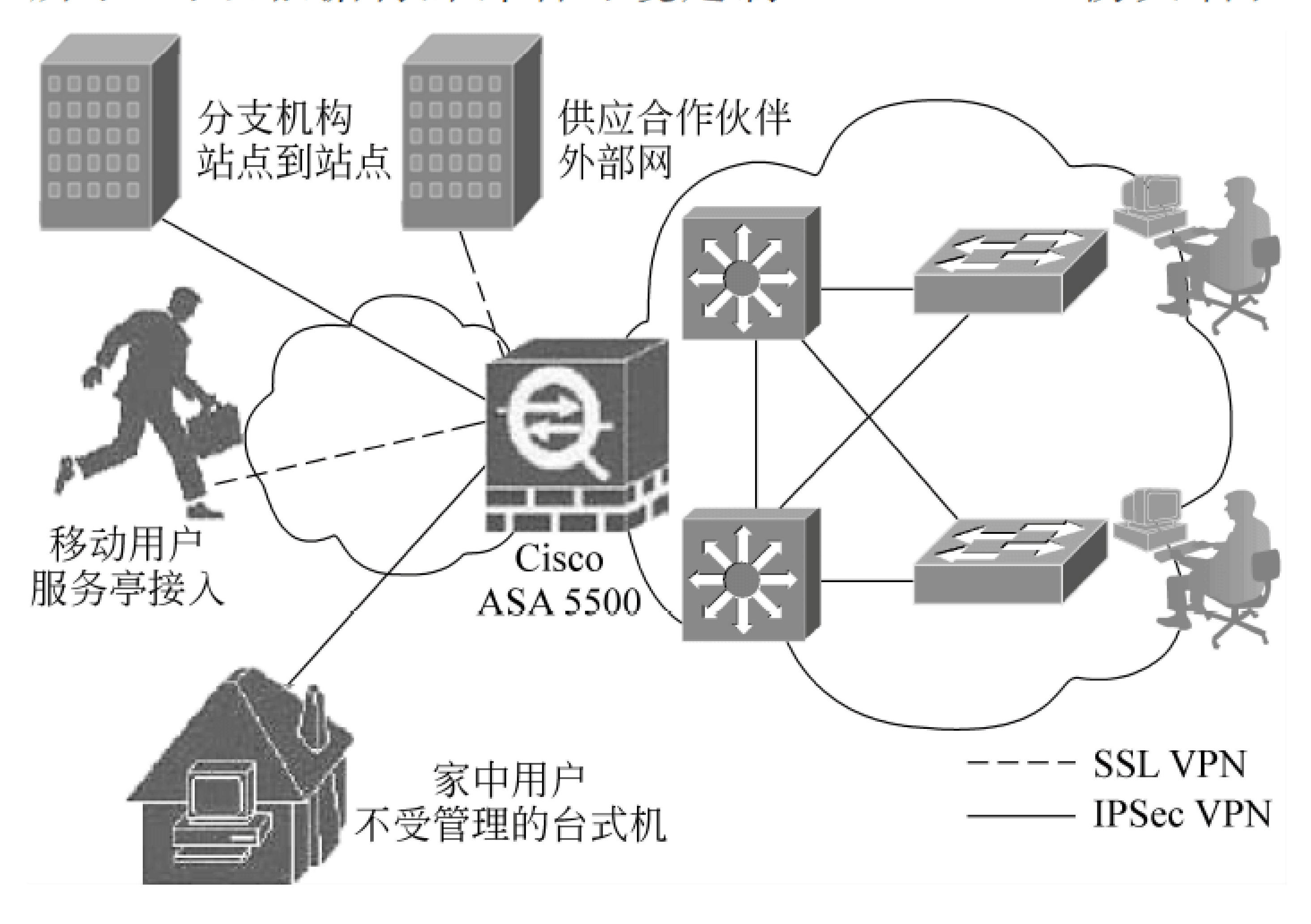


图 9-2　思科 ASA 5500 系列应用体系结构

小企业和分支机构环境中，Cisco ASA 5500 系列商业版还可以作为“一体化”设备，提供全面的威胁防御和 VPN 服务，并满足这种部署的预算和运营要求。

每个版本所满足的特定企业环境需求如下。

（1）防火墙版。使企业能够安全、可靠地部署关键业务应用和网络。独特的模块化设计能够提供卓越的投资保护，降低运作成本。

（2）IPS 版。通过一组防火墙、应用安全性和入侵防御服务，防止关键业务服务器和基础设施遭受蠕虫、黑客及其他威胁的袭击。

（3）Anti-X 版。利用全面的安全服务套件，为小型站点或远程站点的用户提供保护。企业级防火墙和 VPN 服务提供到公司网络的安全连接。来自 Trend Micro 的业内领先的 Anti-X 服务能够防止客户端系统遭受恶意 Web 站点以及病毒、间谍软件和诱骗等基于内容的威胁侵袭。

（4）SSL/IPSec VPN 版。使远程用户能够安全地访问内部网络系统和服务，为大型企业部署支持 VPN 集群。安全套接字层（SSL）和 IP Security（IPsec）VPN 远程接入技术将 Cisco Secure Desktop 等威胁迁移技术与防火墙和入侵防御服务有机结合在一起，保证 VPN 流量不会给企业带来威胁。

1）型号

Cisco ASA 5500 系列包括 Cisco ASA 5505、5510、5520、5540 和 5550 自适应安全设备——这些定制的高性能安全解决方案充分利用了思科系统公司在开发业界领先、屡获大奖和 VPN 在解决方案方面的丰富经验。该系列集成了 Cisco PIX 500 系列安全设备、Cisco IPS 4200 系列传感器和 Cisco VPN 3000 系列集中器的最新技术。Cisco ASA 5500 系列产品性能的比较如表 9-1 所示。

表 9-1　Cisco ASA 5500 系列产品性能的比较

Cisco ASA 5500 系列型号/许可证		Cisco ASA 5505 Base/Security Plus	Cisco ASA 5510 Base/ Security Plus	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
市场		SOHO/ROBO/ MSSP/企业 远程员工	中小企业和小型企业	小型企业	中型企业	大型企业
性能总结	最高防火墙吞吐量(Mbps)	150	300	450	650	1200
	最高 3DES/AES VPN 吞吐量(Mbps)	100	170	225	325	425
	最高站点到站点和远程访问 VPN 用户会话数	10/25	250	750	5000	5000
	最高 SSL VPN 用户会话数	25	250	750	2500	5000
	最高连接数	10000/25000	50000/130000	280000	400000	650000
	新建连接数 /秒	4000	9000	12000	25000	36000
	每秒数据包数(64 字节)	85000	190000	320000	500000	600000

续表

Cisco ASA 5500 系列型号/许可证		Cisco ASA 5505 Base/Security Plus	Cisco ASA 5510 Base/Security Plus	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
技术总结	内存/MB	256	256	512	1024	4096
	集成式端口	28 端口 10/100 交换机，带两个以太网供电端口	5 个 10/100	4 个 10/100/1000，1 个 10/100	4 个 10/100/1000，1 个 10/100	8 个 10/100/1000，1 个 10/100
	最高虚拟接口(VLAN)	3(中继关闭)20(中继启用)	50/100	150	200	250
特性	应用层安全性	有	有	有	有	有
	L2 透明防火墙	有	有	有	有	有
	IPSec 和 WebVPN 服务	有	有	有	有	有
	VPN 集群和负载均衡	未知	未知	有	有	有

2）产品特点

Cisco ASA 5500 系列将 Cisco PIX、IPS 4200 和 VPN 3000 平台经过市场验证的特性集与 Trend Micro 开发的网络 Anti-X 功能集成在同一个设备和管理框架中。这些特性融合之后，产生了新功能，例如，为远程接入 VPN 连接提供蠕虫、病毒和恶意软件防御，在网络周边有效预防各种蠕虫、病毒和恶意软件，以及实施内部和增强应用检测和控制等。因此，与思科推出的专用安全和 VPN 设备相比，Cisco ASA 5500 系列能够提供很多来自于高度融合、相互补充服务的扩展功能。

Cisco ASA 5500 系列设备提供的广泛威胁防御功能还能加强网络防御，无论威胁来自远程机构、总部 DMZ 还是网络内部，都能有效保护网络不受侵害。在经常被忽略的网络部分区域，例如，经济上或运营上不适合部署高级安全功能的远程站点和网络内部，可以利用这种方式消除蠕虫、病毒和恶意软件，提高应用安全性。从这个角度来看，Cisco ASA 5500 系列能够提高整个网络的安全性，进而增强网络安全链的强度。

从现有部署集成的角度来看，Cisco ASA 5500 系列与原先安装的所有 Cisco PIX、IPS 4200 和 VPN 3000 完全兼容。由于这些设备都是利用经过市场验证的相同技术开发的，因此 Cisco ASA 5500 系列与专用设备之间不存在特性差别。不仅如此，部署 Cisco ASA 5500 系列时，安全人员还可以利用与 Cisco PIX、IPX 4200 和 VPN 3000 设备相同的培训内容和知识。

融合型和专用型 VPN 部署都可起到保护当今网络的作用。决策时，应主要考虑网络的规模、网络的架构、在网络中的位置以及 IT 支持方式。Cisco ASA 5500 系列高度灵活，可以同时满足融合型和专用型 VPN 部署的要求。

在网络中统一由 Cisco ASA 5500 系列支持多种部署环境和提供各种安全功能，能够简化网络架构，从而降低部署和运营成本。Cisco ASA 5500 系列非常适合取代 Cisco PIX 515E 和 PIX 525 安全设备，以及由 Cisco VPN 3000 系列集中器提供的 SSL 和 IPSec VPN 服务。由于 Cisco ASA 5500 系列采用了 Cisco PIX 和 VPN 3000 系列的技术，因

此,它提供的所有特性/功能都能与现有的 Cisco PIX 和 VPN 3000 部署兼容。而对于独立式 IPS 部署,Cisco IPS 4200 系列仍然是首选平台。对于 SOHO 和大型总部的传统防火墙和站点间 VPN 部署,Cisco PIX 501、PIX 506E 和 PIX 535 安全设备不但是最经济有效的平台,也可对多站点 Cisco ASA 5500 系列进行有效补充。

2. Cisco VPN 3000 系列集中器

如图 9-3 所示,Cisco VPN 3000 集中器系列由通用的远程访问虚拟专网(VPN)平台和将高可用性、高性能和可扩展性与当今最先进的加密和认证技术结合在一起的客户机软件组成。利用 Cisco VPN 3000 集中器系列,客户可以充分发挥最新 VPN 技术的优势,极大地降低了通信费用。特别地,该产品是业界唯一能够提供现场可更换和客户可升级部件的可扩展平台。这些称为可扩展加密处理(SEP)模块的部件使用户可以轻松地增加容量和吞吐量。



图 9-3　Cisco VPN 3000

外观尺寸(长×宽×高):368.3×444.5×88.9mm;网络协议:IPSec、PPTP、L2TP、L2TP/IPSec、NAT 透明 IPSec;电源电压(V):100-240V;应用级别:SSL VPN。

企业一般使用虚拟专网(VPN),在公共互连基础设施上建立安全、端到端的专用网络连接。目前,VPN 已经成为远程访问连接的首选解决方案,因为部署一种远程访问 VPN,使企业可以利用 Internet 服务提供商提供的本地拨号基础设施来降低通信费用。远程访问 VPN 使移动办公人员、远程办公人员和加班人员能够充分发挥宽带连接的优势。为了完全发挥高性能、远程访问 VPN 的优势,公司必须部署一种健壮、高可用性的 VPN 解决方案,最好是同时使用专用的 VPN 设备。Cisco VPN 3000 集中器系列是适用于企业部署的最佳远程访问 VPN 解决方案,该方案包括一种基于标准的易用 VPN 客户机和可扩展的 VPN 隧道终端设备,还包括一种使企业对自己的远程访问 VPN 实施轻松安装、配置和监视的管理系统。将最先进的高可用性能力与专门构建的远程访问体系结构结合在一起,Cisco VPN 3000 集中器使企业能够构建高性能、可扩展和稳健的 VPN 基础设施,支持自己的关键业务远程访问应用。它是目前业界唯一的一种能够现场更换部件,并由客户完成升级的可扩展平台。这些称为可扩展加密处理(SEP)模块的可更换部件,使用户可以轻松地增加容量和吞吐量。Cisco VPN 3000 集中器支持各种 VPN 客户机软件,包括 Cisco VPN 客户机、Microsoft Windows 2000 L2TP/IPsec 客户机和用于 Windows 95、Windows 98、Windows NT 4.0 和 Windows 2000 的 Microsoft PPTP。

1) 型号

Cisco 客户可以在众多的 VPN 3000 集中器中选择最适合自己需求和应用的具体型号,这些型号支持各种企业客户,包括从只有不到 100 个远程访问用户的小公司到有多达 10000 名用户同时远程访问的大型机构。不论 Cisco VPN 3000 集中器的哪一种版本,都可以在不增加更多费用的情况下提供 Cisco VPN 客户机,并给予不受限制的安装许可证。Cisco VPN 3000 集中器提供非冗余和冗余两种配置,允许客户构建最稳健、最可靠和经济高效的网络。另外还提供高级路由功能,如 OSPF、RIP 和网络地址转

换(NAT)。

Cisco VPN 3000 集中器具有 5 种不同型号,满足各种业务需要。

(1) Cisco VPN 3005 集中器。Cisco VPN 3005 集中器是一种专为中小规模组织机构设计的 VPN 平台,能够满足带宽要求高达 T1/E1(4 Mbps 最大性能)的全双工和多达 100 个的同时对话,加密处理由软件完成。但 Cisco VPN 3005 本身不支持升级功能。

(2) Cisco VPN 3015 集中器。Cisco VPN 3015 集中器是一种专为中小规模组织机构设计的 VPN 平台,能够满足带宽要求高达 T1/E1(4 Mbps 最大性能)的全双工和多达 100 个的同时对话。同 Cisco VPN 3005 一样,加密处理由软件完成,不过 Cisco VPN 3015 可现场升级为 Cisco VPN 3030 和 3060。

(3) Cisco VPN 3030 集中器。Cisco VPN 3030 集中器是一种专为中型、大型组织机构设计的 VPN 平台,能够满足带宽要求从 T1/E1 到 T3/E3(50Mbps 最大性能)的全双工和多达 1500 个人的同时对话。专用的 SEP 模块完成基于硬件的加速处理功能。Cisco VPN 3030 可现场升级到 Cisco VPN 3060,另外还提供冗余和非冗余两种配置。

(4) Cisco VPN 3060 集中器。Cisco VPN 3060 集中器是一种专为需要最高性能和可靠性的大型组织机构设计的 VPN 平台,能够满足带宽要求从部分 T3 到完全 T3/E3 甚至更高(100Mbps 最大性能)和多达 5000 个同时对话。专用的 SEP 模块完成基于硬件的加速处理功能,另外 Cisco VPN 3060 还提供冗余和非冗余两种配置。

(5) Cisco VPN 3080 集中器。Cisco VPN 3080 集中器为那些需要最高性能的大型企业进行过专门优化,能够支持多达 10000 个的同时远程访问对话。专用的 SEP 模块完成基于硬件的加速处理功能。另外 Cisco VPN 3060 只提供全冗余配置。

(6) Cisco VPN 客户机。易于部署和操作的 Cisco VPN Client(Cisco VPN 客户机)用于建立到 Cisco VPN 3000 集中器的安全的、端到端的加密隧道。这种采用遵循 IPSec 的简化设计思想的客户机随 Cisco VPN 3000 集中器一同提供,并对用户数量不予限制。Cisco VPN 客户机可以预先设置成大量部署状态,在最初登录时,用户需要干预的内容很少。VPN 访问策略在 Cisco VPN 3000 集中器内创建并集中保存,当与客户机建立连接时,自动发往客户机。

2) 产品特点

(1) 高性能、分布式处理体系结构。

① Cisco SEP 模块提供基于硬件的加密功能,保证了在整个额定容量中保持一致的性能(Cisco VPN 3030-3080)。

② 大规模隧道提供了 IPSec、PPTP 和 L2TP/IPSec 连接。

(2) 可扩展性(Cisco VPN 3015-3060)。

① 模块化设计(4 个扩展槽)实现了有效的投资保护、冗余和简单的升级途径。

② 系统体系结构的设计原则提供一致、高可用性的性能。

③ 所有的数字设计都实现了最高可靠性和 24 小时的不间断工作。

④ 健壮的测量测试程序提供了正常工作期间的监视和告警功能。

⑤ 与 Microsoft 的兼容性使大规模部署客户机软件和与相关系统进行无缝集成成为可能。

(3) 安全性。

① 完全支持现有和最新安全标准,允许与外部认证系统集成,并可以与第三方产品相互操作。

② 具备动态数据包过滤和地址转换的防火墙可以提供企业 LAN 所需要的安全功能。

③ 用户和用户组一级的管理实现了最大的灵活性。

(4) 高可用性。

① 冗余子系统和多机箱故障切换能力保证了最大的系统正常运行时间。

② 丰富的测量测试和监视功能为网络管理员提供了实时监视系统状态和进行早期告警的能力。

(5) 稳健的管理特性。

① Cisco VPN 3000 集中器可以使用标准的 Web 浏览器(HTTP 或 HTTPS),或通过 TELNET、安全 TELNET、SSH 和控制台端口进行有效管理。

② 企业和服务提供商都能得到配置和监视能力。

③ 访问级别由用户或用户组来配置,这样安全策略的配置和维护就非常容易。

3. Cisco VPN 路由器

目前,所有的 Cisco 路由器平台都可以方便地实现 VPN。经过优化的 Cisco 路由器集成了 VPN 功能、高速加密、安全、带宽管理和与 WAN 连接的能力,降低了 VPN 的复杂度和成本。该产品系列包括用于企业和地区办公环境的 Cisco 7500、7200VXR 和 7200 高端路由器,以及用于小型地区、分支机构及远程个人的 Cisco 3600、2600、1720 和 800 路由器。所有的 Cisco VPN 路由器都完全可以互操作,为从园区到广域网 ISP,以窄带或宽带速率进行多媒体通信提供了一条可扩展的端到端链路。

1) IPSec VPN 服务模块

为 Cisco Catalyst 6500 系列和 Cisco 7600 系列互联网路由器设计的 IPSec VPN 服务模块基础设施集成式高速 VPN。关键的高带宽企业应用推动了大型机构对无所不在的连接性和更高带宽的需求。许多企业正利用站点间虚拟专用网(VPN)来强化或替代其传统 WAN,以便更好地满足上述新连接需求。

(1) 产品特点。Cisco IPSec VPN 服务模块能够为 Cisco Catalyst 6500 系列和 Cisco 7600 系列互联网路由器上的端点位置提供经济有效的 VPN 性能,详见表 9-2。Cisco IPSec VPN 服务模块提供的主要特性如下。

① 能集成到网络基础设施中:模块同时支持 Cisco Catalyst 6500 系列和 Cisco 7600 系列互联网路由器。由于 VPN 集成在这些基础设施平台中,无须另外添置设备和网络组件就能提高网络安全性。不仅如此,全部网络服务模块都能与安全基础设施一起使用。

② 高性能和可扩展性：这个模块利用了最新的加密硬件加速技术，能够为大型分组（500 字节以上）提供 1.9Gpbs 的 3DES 流量，为普通大小的分组（300 字节）提供 1.6Gbps 的 3DES 流量。另外，它不但能同时端接 8000 条 IPSec 通道，还能以高于当前产品的速度设置这些通道。

③ 提供高级安全服务：推出 IPSec VPN 模块后，为网络添加加密、认证和完整性功能变得更加容易。安全园区网、供应商边缘 VPN 终止和安全融合网络服务（如 VoIP 和存域网）等应用非常易于部署。

表 9-2 Cisco IPSec VPN 服务模块特性

要　　求	特点/优势
高速 VPN 性能	大型分组的 IPSec 吞吐量高达 1.9Gbps 3DES，300 字节分组的吞吐量高达 1.6Gbps
将 VPN 集成到基础设施中	VPN 模块支持 Cisco Catalyst 6500 机箱，因而允许用集成式方法在基础设施中建立 VPN。无须在园区网、内部网和/或城域网中使用独立的 VPN 设备
全套 VPN 特性	多种 PKI 支持，自动登记证书以及全套通道支持
适应多种网络流量类型和网络拓扑	借助 Cisco IOS 软件，几乎可以安全、可靠地传输任何类型的网络流，包括在 IPSec VPN 上传输多协议、组播和 IP 电话。不仅如此，丰富的路由功能还允许使用网状和分级网络监控
保证长 VPN 开机时间	通过 IPSec、IKE 保持激活信息、HSRP 和环境监控路由
VPN 和网络基础设施管理	VPN 管理分成两类： • 针对单设备管理的嵌入式 HTML VPN Device Manager（VDM） • 针对服务供应商和大企业 VPN、安全性和 QoS 管理的 VPN Solution Center（VPNSC）

2）技术指标

（1）VPN 隧道：

IPSec（IP Security-RFC 2401-2411，2451）。

（2）加密：

ESP DES 和 3DES（RFC 2406，2451）。

（3）认证：

① x.509 数字证书（RSA 签名）；

② 共享密钥；

③ 简单证书登记协议；

④ RADIUS（RFC 2138）；

⑤ TACACS+；

⑥ CHAP/PAP（RFC 1994）。

（4）完整性：

HMAC-MD5 & HMAC-SHA-1（RFC 2403-2404）。

(5) 密钥管理：
① 互联网密钥交换(RFC 2407-2409)；
② IKE-XAUTH；
③ IKE-CFG-MODE。
(6) 证书认证：
① Entrust；
② VeriSign；
③ Microsoft；
④ IPlanet；
⑤ Baltimore Technologies。
(7) 弹性：
① 热备份路由器协议(HSRP)；
② IKE 保持激活信息；
③ IPSec 路由。
(8) 管理选项：
① VPN Device Manager (VDM)预载；
② Cisco Works 2000；
③ 使用安全套接层(SSH)或 kerberized telnet 的安全命令行界面。
(9) 路由协议：
① BGP4；
② RIP/RIP2；
③ OSPF；
④ EIGRP IGRP；
⑤ IS-IS。
(10) 嵌入式接口：
无。
(11) 模块支持：
① 所有 Cisco Catalyst 6500/Cisco 7600 GE & FE 接口模块；
② MSFC2/SUP2。

9.1.2 Array SPX 系列 SSL VPN 访问网关

Array Networks 是一家应用智能安全公司，致力于为用户提供多层网络安全和应用解决方案。通过智能化的集成，Array Networks 所提供的无客户端的 SSL VPN 安全产品平台及应用加速网络流量管理平台能够极大简化网络架构，增强网络应用的性能。

Array Networks SSL VPN 访问网关可以让企业员工、客户和合作伙伴随时随地安全访问企业的商业机密信息，从而提高公司的生产效率，降低 IT 成本。作为专门提供高

性能接入控制的安全产品，SPX系列可以为远程和本地的用户提供可扩展的接入能力，同时保证最强的安全性和最短的应用响应时间。

1. 产品特点

(1) 应用支持。SPX系列通过多种卓越的技术，实现对企业的各种业务应用的访问，无论是B/S结构应用还是C/S结构应用，底层数据都经过SSL协议安全防护，充分满足了企业业务应用的全面安全访问需求。

(2) 领先的整体性能。对内外网络用户的访问控制越来越广泛地被部署，不但应用到企业的远程办公环境中，还会应用到企业的业务系统中，访问量会非常大。Array SPX系列通过多种独特技术保障系统的整体性能。Array具有业界领先的处理性能和容量指标，最大支持并发用户数达64000个。

(3) 访问控制。对企业数据中心和业务应用的安全威胁，很大一部分是非授权的访问，因此认证授权对于访问控制至关重要。Array SPX系列提供多种认证手段和细粒度的授权访问策略，保障对企业业务应用访问的可控性和安全性。

(4) 端点安全。外网的SSL VPN用户一般是通过互联网接入，接入的客户端千奇百怪，这些客户端不在企业内部网络中，不具备企业统一的安全防护策略，可能为不法分子掌控，或者感染了恶意代码；内网用户的客户端也由于各种原因普遍存在安全漏洞。Array SPX系列通过端点安全功能来消除这些给企业数据中心、关键业务应用带来的安全隐患。

Array Networks产品的其他特点详见表9-3。

表9-3 Array Networks产品的特点

功 能	特 点 描 述	客 户 价 值
无客户端安全访问	客户端只需要具备标准浏览器即可使用SSL VPN，不需要预装专用的客户端软件	用户可以随时随地、方便、安全访问企业的内部应用，提高企业的生产效率
虚拟化技术	提供多达256个的虚拟门户，每个门户可以具有自己的域名、IP地址、认证授权策略和独享的内部网段。支持VLAN绑定和IP地址重叠。支持自定义的门户界面，支持中文门户界面	可以为企业不同的组织分配不同的访问入口，做到更高的用户隔离、网络隔离、资源隔离，提高整体安全性
WebDirect-Web Resource Mapping	通过WebDirect Proxy，客户端可以访问内部的Web资源。支持改写Web内容，掩藏内部URL和IP地址，达到更高的安全保护。支持各种类型的客户端，如Windows、Linux、Cell Phone、PDA等	100%无客户端访问内部Web资源，通过认证、加密、七层控制，达到更高的安全性，且不需要安装任何插件和控件。更加灵活便捷，使企业Web应用接入管理和部署更加轻松
WebDirect-File Sharing	提供客户端对内部的文件共享服务器的浏览、删除、上传、下载操作，支持SMB/DFS(Windows)、NFS(UNIX)，支持源服务上的访问权限控制	通过SSL VPN的Web浏览器方式访问内部文件服务器，使远程安全上传、下载内部机密文件更加方便简易

续表

功　能	特 点 描 述	客 户 价 值
Array OS 具有专门设计的 SpeedStack 系统架构	反向代理引擎完全隔离所有外部数据请求和内部数据请求；独有的 TCP/IP 协议栈、实现 TCP/IP 数据在系统中只处理一次，杜绝了重复性作业	通过特殊堆栈，更有效地处理数据包，从而获得更高性能。由于不用再作重复性数据处理，因而获得了更多用于处理其事务的处理能力
Connect Multiplexing	把许多客户端单独的 HTTPS 请求捆绑到相对较少的与服务器的 TCP 连接中，而不用采用一对一的方式，把每一个 TCP 连接从客户端传递到服务器	减少服务器的负载，提高应用的响应能力
SSL 硬件加速	通过 SSL 硬件加速卡实现 SSL 运算，具有极高的 SSL 处理能力，实现内核级的密钥交换和批量加密，保证系统响应毫秒级的延迟。支持端到端的 SSL 加密	具有行业领先的 SSL 性能指标，大幅缩短用户等待时间，增强了 SSL VPN 响应能力，极大提高了企业关键应用的访问体验，保证企业生产的高效率
HTTP 压缩	支持硬件 HTTP 压缩，符合 HTTP 标准压缩规范。自动识别客户端对压缩算法的支持，并依次实现动态压缩	节省用户带宽，缩短用户下载内容的时间，提高 Web 应用访问的响应质量
并发用户处理能力	最高端的设备可以支持多达 64000 个并发用户	降低用户的硬件成本，更方便扩展为企业级的实施方案，同时使每个并发用户的成本最低
LocalDB 认证	SPX 设备内部有一个小型数据库，可以存放用户名和密码信息	不需额外的认证服务器即可实施网络接入认证，便于系统的快速部署
第三方认证服务器	支持 Radius、LDAP、AD 等第三方认证服务器的用户身份认证，并可在多个认证服务器中顺序查找	便于和企业已有的认证系统集成，企业可以统一管理用户接入
数字证书验证	支持客户端数字证书验证，并可以验证证书内部主题字段，数字证书可以存储在智能卡、USB-Key 等介质中	和 PKI 架构相结合，极大地提高系统接入的安全性
基于特定因素的认证	可以设定允许登录的时间和日期，检测客户端的网络端口 MAC 地址、硬盘序列号等硬件信息，并与用户的身份信息比对，确定其接入权限	限定用户访问应用的时间段，使用指定的客户端硬件平台访问关键业务应用，增强安全度
Host Checking 客户端安全检查	检测客户端的相关状态、信息，赋予不同的接入权限。如检测客户端 IP 地址、注册表、特定文件、应用进程、防病毒软件和个人防火墙软件设置及代码库更新、操作系统版本及补丁，支持客户自定义的一些检测规则	通过检测客户端安全状态及实施相应权限控制，降低客户端非安全因素对数据中心的安全影响，保障企业网络、应用的安全性

2. 产品型号

产品类型：SPX 1800/2800/3800/4800/5800/6800，各产品性能如表 9-4 所示。

表 9-4 SPX 系列产品性能

	SPX 1800	SPX 2800	SPX 4800	SPX 5800	SPX 6800
端口配置	固定端口 4 × 10/100/1000Base-TX	固定端口 4 × 10/100/1000Base-TX	固定端口 4 × 10/100/1000Base-TX	4 个端口：2 × 10/100/1000Base-TX＋2×1000Base-SX 或者 4 × 10/100/1000Base-TX	4 个端口：2×10/100/1000Base-TX＋2×1000Base-SX 或者 4×10/100/1000Base-TX 或者 2×10/100/1000Base-TX＋2×10G Fiber
SSL 处理	硬件卡	硬件卡	硬件卡	硬件卡	硬件卡
最大并发用户数	100	1200	6000	12000	64000
集群	32	32	32	32	32
尺寸	1U；标准 19″机柜；17″(宽)，15″(长)，1.75″(高)	1U；标准 19″机柜；17″(宽)，15″(长)，1.75″(高)	1U；标准 19″机柜；17″(宽)，15″(长)，1.75″(高)	2U；标准 19″机柜；17″(宽)，21.5″(长)，3.5″(高)	2U；标准 19″机柜；17″(宽)，21.5″(长)，3.5″(高)
控制端口	Male DB9 系列(RS232)端口	Male DB9 系列(RS232)端口	Male DB9 系列(RS232)端口	Male DB9 系列(RS232)端口	Male DB9 系列(RS232)端口
重量/磅	13.6	13.6	13.6	30	30
电源	100～240VAC，47～63Hz，3A，Auto-ranging	100～240VAC，47～63Hz，3A，Auto-ranging	100～240VAC，47～63Hz，3A，Auto-ranging	100～240VAC，50～60Hz，2～4A，Auto-ranging，冗余电源，热插拔	100～240VAC，50～60Hz，2～4A，Auto-ranging，冗余电源，热插拔
环境	操作温度：0°～40°C；湿度：0%～90%；无冷凝	操作温度：0°～40°C；湿度：0%～90%；无冷凝	操作温度：0°～40°C；湿度：0% ～90%；无冷凝	操作温度：0°～40°C；湿度：0%～90%；无冷凝	操作温度：0°～40°C；湿度：0%～90%；无冷凝
规范依从	电磁辐射：FCC、ICES、VC-CI、MIC、BSMI、AS/NZS 3548、EN 55022、EN 55024 Class A；EN 60950，UL 1950，CAN/CSA 950，NOM	电磁辐射：FCC、ICES、VC-CI、MIC、BSMI、AS/NZS 3548、_EN 55022、EN 55024 Class A；EN 60950，UL 1950，CAN/CSA 950，NOM	电磁辐射：FCC、ICES、VC-CI、MIC、BSMI、AS/NZS 3548、_EN 55022、EN 55024 Class A；EN 60950，UL 1950，CAN/CSA 950，NOM	电磁辐射：FCC、ICES、VC-CI、MIC、BSMI、AS/NZS 3548、_EN 55022、EN 55024 Class A；EN 60950，UL 1950，CAN/CSA 950，NOM	电磁辐射：FCC、ICES、VCCI、MIC、BSMI、AS/NZS 3548、_EN 55022、EN 55024 Class A；EN 60950，UL 1950，CAN/CSA 950，NOM
安全规范	CSA，CE，UL，C/US	CSA，CE，UL，C/US	CSA，CE，UL，C/US	CSA，CE，UL，C/US	CSA，CE，UL，C/US
平均无故障时间/年	5	5	5	5	5

9.1.3 Juniper Networks SA 系列 SSL VPN 访问网关

Juniper Networks(瞻博网络)公司致力于实现网络商务模式的转型。作为全球领先的联网和安全性解决方案供应商,Juniper Networks 公司对依赖网络获得战略性收益的客户一直给予密切关注。公司的客户来自全球各行各业,包括主要的网络运营商、企业、政府机构以及研究和教育机构等。Juniper Networks 公司推出一系列联网解决方案,提供所需的安全性和性能,来支持全球最大型、最复杂、要求最严格的关键网络。

如图 9-4 所示,Juniper Networks SA 系列 SSL VPN 以完整的远程接入应用,在 SSL VPN 市场保持领导地位,其产品包括具有高扩展性和冗余功能的、专门为大型企业和电信运营商而设计的全新下一代 Juniper Networks SA2500、SA4500 和 SA6500 SSL VPN。SA 系列把 SSL 的安全性与基于标准的接入控制、粒状策略制定和无可比拟的灵活性结合起来。其结果是采用极其严格的接入控制选项,为所有企业提供全面的安全性,以保护其最敏感的应用和数据。与传统的 IPSec 客户端解决方案相比,Juniper Networks SA 系列 SSL VPN 的总体拥有成本更低,并提供独特的端到端安全特性。



图 9-4 Juniper Networks SA 系列产品

1. 产品特点

(1) 市场领先的单一 SSL VPN 安全平台,满足所有的远程接入需求。
(2) 无客户端访问企业应用和资源。
(3) 一流的端点安全性、细粒度的访问控制和威胁防御功能。
(4) 可扩展的产品,为各种规模的公司提供远程和外联网访问支持。
(5) 面向电信运营商的高度可用、高可扩展的产品。

表 9-5 Juniper Networks SA 系列产品优势

特　性	优　势
使用 SSL	安全远程接入,无须部署任何客户端软件部署,无须进行维护,也无须改变现有服务器
跨平台支持	提供出色灵活性,允许用户使用任何类型的操作系统,从任何类型的设备访问公司资源
主机检查器	扫描端点,确保在会话前和会话中均符合公司安全政策
单点登录(SSO)功能	减少最终用户输入和维护多个接入权限的需要
资源授权	允许管理员为特定群体定制安全政策,使其只能访问必要数据
UAC-SA Federation	允许本地或远程用户通过一次登录即可无缝访问受到 UAC 或 SA Series 的访问控制政策保护的公司资源,从而可以有效简化最终用户的体验

2. 产品型号

Juniper Networks SA 系列产品型号如表 9-6 所示。

表 9-6 Juniper Networks SA 系列产品型号

产品	目标市场	企业级特性
SA700	中、小型企业	无须任何客户端软件，就能为远程或移动员工提供安全接入 可以利用任选升级功能，从任何地方的任意 PC 接入 即插即用部署 强大的安全特性
SA2000	中、小型企业	为员工、业务合作伙伴和用户提供安全的局域网、内联网和外联网接入 3 种接入方法，使管理员能够按用途提供接入 动态访问权限管理 高级软件支持高级功能，包括利用 Centeral Manager 简化管理统一标准认证
SA2500	中、小型企业	支持部署经济高效的远程和外联网接入方案，以及内联网安全方案 用户可以以 Web 形式，从任意机器访问企业网络和应用 提供高可用性（HA）和无缝的用户故障切换功能 即使是规模较小的机构，也能够获得同样的高性能、管理的灵活性和用户体验 在一个系统或双机群集上处理 100 个并发用户
SA4000	大、中型企业	可以扩展的平台使大型企业能够从一个平台提供安全的外联网、内联网和局域网接入 企业性能/高可用性 基于许可证的 SSL 加速和针对所有流量类型的压缩 动态访问权限管理，提供 3 种接入方法 统一标准认证，支持 FIPS 设备 高级软件支持高级功能，包括利用 Central Manager 简化管理
SA4500	大、中型企业	通过 Web 浏览器，就可为远程员工和合作伙伴提供经济高效的外网接入服务 具有全面的访问权限管理功能，可用于创建安全的客户/合作伙伴外网接入，并允许企业安全地访问公司内网，从而使不同员工和访客能够在遵循企业安全策略的同时准确地使用所需的资源 面向各种流量的内置压缩功能可提高性能；对于要求更严格的环境，还可提供基于硬件的 SSL 加速功能 提供高可用性和无缝的用户故障切换功能
SA6000	大型和跨国企业	为最大、最复杂、最安全的外联网、内联网和局域网接入部署 提供高性能平台 为所有流量类型提供内置 SSL 加速和压缩 冗余和/或可热插拔的硬盘、电源和风扇 动态访问权限管理，提供 3 种接入方法 统一标准认证、支持 FIPS 设备 高级软件支持高级功能，包括利用 Central Manager 简化管理
SA6000 SP	电信运营商托管服务	实施了全面虚拟化的 SSL VPN 平台，使 SP 能够从一台设备或一个集群为多家规模各异的企业提供基于网络的 SSL VPN 服务 不需要安装客户端，不会发生防火墙或 NAT 穿越问题，因而不会加重支持负担，增加 ROI 通过提供外联网接入、灾难恢复、内联网和局域网安全性、移动设备接入等服务创造异化收入机会 多种特性满足电信运营商对性能、可扩展性和高可用性的要求

9.1.4 F5 Networks

在全球应用流量管理领域中,F5 Networks 公司是网络流量管理方面的领先厂商。通过为应用型网络提供开放式互联网控制结构,F5 为业界提供先进的成套集成产品和服务,使用户能够在互联网流量方面进行管理、控制和优化。

F5 的产品不仅能够帮助网络用户消除因为带宽而产生的拥堵或堵塞,而且能够极大地提高执行诸如 Web 出版、电子商务、防火墙等关键任务的互联网服务器和相关应用系统的可用性和速度。F5 的解决方案被广泛地部署于全球的一些大型企业、领先的服务供应商、金融机构、电信、政府机构和门户网站的网络建设中。

F5 的 VPN 设备主要是 FirePass 产品系列。

FirePass 1200 系列。FirePass 1200 控制器是专为中小型企业精心设计的 1U 机架安装式服务器。它支持 10～100 个并发用户,为基于 Web 方式安全远程访问企业应用和桌面提供了一套全面的解决方案。

FirePass 4100 系列。FirePass 4100 控制器是专为大中型企业精心设计的 2U 机架安装式服务器。它可支持多达 2000 个并发用户,为基于 Web 方式安全远程访问企业应用和桌面提供了一套全面的解决方案。

FirePass 4300 系列。FirePass 4300 控制器是专为大中型企业和运营商精心设计的 2U 机架安装式服务器。它支持多达 2000 个并发用户,采用四核 CPU 获得最佳性能。此外,FirePass 4300 还支持内置的冗余电源和可选的千兆光纤端口。

9.2 国内主流产品

9.2.1 深信服 SINFOR M5100-S

如图 9-5 所示,深信服 M5100-S 路由器是面向中小企业、区域总部推出的百兆 VPN 产品;可以部署在中小企业的网络中心,也可以部署在大型企业较大分支机构的网络中心。该产品集成 IPSec VPN、SSL VPN、防火墙功能。M5100-S 的 IPSec VPN 功能可以低成本地实现和远程分支结构的网间互连;而 SSL VPN 功能则最适合移动办公人员和合作伙伴的远程安全接入,防火墙功能还可以有效保证企业网络的 Internet 入口安全。



图 9-5 深信服 M5100-S 系列路由器

深信服 M5100-S 带有 4 个 10/100 Base-T 网络接口(1×LAN、2×WAN、1×DMZ)。IPSec VPN 加密速度(AES 128bit)为 54.4Mbps,SSL VPN 加密速度为 70Mbps,防火墙吞吐量(双向 256 bits)达 95Mbps,支持 1500 条并发 VPN 隧道和 200 个 SSL 并发用户。大容量的设计有效确保用户局域网及 VPN 网络高效稳定地运行。针对带宽及稳定性要求较高的用户,M5100-S 还提供了双 WAN 端口设计,实现了两条 Internet 出口线路的带宽叠

加和备份。同时，基于多线路的智能选路技术，M5100-S有效解决了位于不同网络服务商的移动用户跨运营商访问总部网络时存在的延迟大、带宽小的问题。

9.2.2 联想网御 SJW44(100S)

网御VPN硬件安全网关是独立的VPN网关设备，由高可靠性的工控标准主板、硬件密码模块和电子盘等构成，内置专用嵌入式操作系统和VPN软件模块。

如图9-6所示，联想网御SJW44(100S)路由器带有3个10/100Base-T端口和4个10/100Mbps交换机端口，支持协议包括TCP/IP、UDP、ICMP、IPSEC、IKE。它是一种基于IPSec技术的VPN产品，集专用操作系统、身份认证、信息加密及安全日志审计等功能于一体，提供了可靠、高速、透明的信息加密功能；并且依靠联想在防火墙系列产品上的技术积累，在VPN产品内部嵌入了基本的防火墙功能模块，以防止外部网络对网御VPN加密网关的攻击。用户可以透明地在原有网络架构上构建远程安全接入VPN、企业内部Intranet VPN、企业外延Intranet VPN，从而提供网关到网关、客户端到网关、客户端到客户端的虚拟安全数据信息传输通道。



图9-6 联想网御SJW44(100S)VPN路由器

9.2.3 冰峰网络 Iceflow S5500

冰峰S5500-MC全面覆盖IPSec/SSL的接入应用，并植入MC上网行为管理模块，支持大规模SSL移动接入和IPSec局域网拓展，支持远程镜像加速、虚拟桌面技术、“8+6”策略认证、安全准入控制，主要推动千兆网络企业的中心机构接入，适合结点分布广泛、单一的多用户协同。

如图9-7所示，冰峰ICEFLOW S5500带有网络端口(4个1000Base-TRJ-45端口)、Console(1个DB9端口)、com端口(1个DB9端口)、USB端口(2个)，支持协议包括IPSec/SSL协议，支持Web SSL/Web TSSL/TSSL多方式接入。其特性在于高强度负荷下的安全与稳定，完全移植F5600原型的高端特性，支持Web SSL、Web TSSL、移动TSSL等多种SSL接入方式，支持本地用户数达10000个，并发用户达5000个，使得该产品在高端市场上颇受青睐，是大规模接入用户的首选。在网络接口上，S5500专门增设一个WAN1口，为VPN技术下的多线路智能分流、中转、选路等提供便捷。



图9-7 冰峰S5500-MC路由器

9.3 选购标准

选购最适合企业的VPN产品，除了应该了解企业架构的商业特性之外，还必须对整体网络环境有所了解，才不致错买了不适用的VPN产品，既没达到VPN的功效，又徒然浪费金钱。随着企业组织方式的扁平化发展，企业分布地域日益广泛以及对信息资产安全的日益重视，企业迫切需要一种技术，把原有各个孤立的局域网连为一个整体，以便在全局的网络视图下构筑一个可靠的、安全的网络信息传输和管理平台。随着骨干网络带宽十倍、百倍地提升，以及ADSL、HFC等宽带接入方式的普及，Internet已经成为各种实时关键性应用的良好数据传输载体，而用户的注意力也由原来的关注网络的稳定性、可用性，逐渐集中到联网方案的易用性和安全性上。VPN技术的发展与成熟，为企业的商业运作提供一个无处不在的、可靠的、安全的数据传输网络。一套完整的VPN产品一般包括3个部分：

① VPN网关：用于实现LAN到LAN。

② VPN客户端：与VPN网关一起实现客户到LAN的VPN方案。

③ VPN管理中心：对VPN网关和VPN客户端的安全策略进行配置和远程管理。在选择VPN产品时，可从以下几个方面来考虑。

9.3.1 VPN设备的性能要求

VPN网关通常部署在网络的边界，如果性能不够，就不能充分发挥网络带宽的效用，影响内网用户的上网速度和VPN专网上软件的运行速度。所以，选购何种性能的VPN网关，应该掌握如下4个原则。

(1) VPN网关的“加密吞吐率”大于等于网络的出口带宽，以免在VPN安全网关上产生性能瓶颈。“加密吞吐率”与加密强度有关，通常加密强度越高，安全性更好，但需要更高端性能的产品支持。

(2) 部署在中心结点的VPN网关的“并发隧道数”大于等于并发接入的VPN网关数目(通常部署在分支机构边界)和并发移动用户数目之和。

(3) 部署网络边界的安全网关的“并发会话数”，与本地局域网内的上网PC的数目相关(具体照应关系可咨询安达通机构)。

(4) 对于分支机构分布在全国各地的企业，目前国内国情决定了跨运营商的网络通信速度通常较慢。这样，为确保整个企业专网的快速有效，企业总部通常采用多ISP(网络运营商)线路接入(如一根电信线路、一根网通线路)，部署具备负载均衡功能的VPN网关。外地分支机构可选择最快速的线路接入总部，解决了跨运营商的网络传输速度不佳的问题。负载均衡VPN网关的“加密吞吐率”应该大于各接入线路的带宽总和。

9.3.2 VPN 设备的安全性

VPN 网关的安全性主要来源于以下 4 个方面。

(1) 加密算法的安全性。VPN 技术的保密性主要依赖加密算法的加密,来确保内部信息在公网上传输的安全性(保密性、完整性和不可抵赖性)。在中国境内销售的 VPN 设备,除了支持国际通用的加密算法(如 DES、3DES、AES、SHA、RSA、DH 等)外,必须支持国家密码管理局批准的国产加密算法(如 SCB2 算法等)。根据《中华人民共和国商用密码管理条例》的规定,只有经过国家密码管理局鉴定过的 VPN 产品(如"SJW74"为国家密码管理局批准安达通公司使用的产品型号)才能使用国产加密算法,并得到国家的认可和安全性确保。

(2) VPN 通信结点的认证安全性。为了防止 VPN 信息外泄,还需要确认 VPN 结点的身份合法性。除了"用户名+密码"和 USBKEY 认证等通常认证方式外,还可以采用数字证书、动态口令、短信认证、外挂 Windows AD 等多种认证方式来确保 VPN 通信结点的身份真实性。

(3) VPN 网关的访问控制能力。VPN 设备应当能够对接入用户的访问权限进行控制,保证其只能访问被授权访问的资源,也可以控制是否为单向访问。优秀的 VPN 设备还应支持按照"角色—用户—资源"来进行用户访问控制。

(4) VPN 准入控制能力。最优秀的 VPN 设备具备"接入用户的准入控制能力"。即能够确保接入用户的安全性,杜绝 VPN 内部用户将病毒、木马等威胁程序带进内网。

9.3.3 VPN 设备对使用环境的适应性

成熟的 VPN 产品不仅能够满足基本的 VPN 互联功能,而且便于使用、安全性强、适应性很强,能够在对用户影响最小的情况下快速部署。VPN 设备是否具备下面 5 个方面的高级功能,是其对环境适应能力的重要衡量标准。

(1) 是否具备"单臂连接"功能。即可将 VPN 网关当做一台服务器或主机,只接一个口到内网交换机中,专门处理 VPN 报文的加解密,不需要修改用户网络物理拓扑,不给网络造成额外的单点故障,也不会降低主干网络的性能。

(2) 是否能在网络 IP 地址冲突的情况下部署 VPN,而不用改动用户网络的原有地址。

(3) 能否使异地网络通过 VPN 无缝联入总部,而不修改总部网络中的路由设备。

(4) 是否支持完全透明的"网桥"模式,使设备能够像一段网线一样透明接入用户的网络,并能在网桥模式下建立 VPN 隧道。

(5) 是否支持"隧道接力"技术,即分支机构 VPN 结点之间可以通过中心结点的接力实现相互间的数据中转,进行快速隧道延伸。

不具备这些技术,将可能使用户在安装和使用 VPN 时有非常大的困扰和麻烦。所以,"易用性"和对复杂环境的"适应性"是选购 VPN 的决定性因素之一。

9.3.4 VPN 设备的性价比

IPSec 和 SSL VPN 是当前两种主流的 VPN 技术,各有优势。所以,一台 VPN 设备如果能够支持 IPSec/SSL 合二为一,是最佳选择,综合投入也最小。网关—网关(Site-Site)互连,采用 IPSec 和 IKE 协议;“移动用户—网关”(Clien-TSite)互连,即可采用 SSL 协议或改进型的 SSL 协议(如 IPSec over Https/Http),使用 Internet Explorer 浏览器和 VPN 网关互联,也兼容采用 IPSec/IKE 协议的 VPN 客户端和网关互连。

VPN 安全网关应当集成防火墙功能,可独立充当防火墙使用。

如果 VPN 安全网关可进一步升级成 UTM 网关或 TPN 网关,并只需要支付差价即可获得这种服务,那么这类 VPN 产品就更具价值,可保障用户投资长期受益。

9.3.5 VPN 网络的可管理性

在构建大规模 VPN 网络时,VPN 的网络管理非常重要。好的 VPN 产品应该配套有完善的 VPN 网络管理系统,涵盖 VPN 策略的集中管理和自动分发、VPN 结点监控、流量统计、日志报表等各种网管功能。

另外,对于大型 VPN 网络,为确保 VPN 结点的身份真实性,最好的方法之一就是采用数字证书(CA)认证服务。优秀的 VPN 产品不仅需要支持第三方 CA 颁发的数字证书,而且是否具有自主知识产权的数字证书认证产品,以及该产品是否成熟、是否能和 VPN 产品无缝整合,也是衡量一个 VPN 厂商实力是否雄厚的重要标准之一。

9.3.6 VPN 设备的资质和制造商资质

《中华人民共和国商用密码管理条例》中规定,“商用密码技术属于国家秘密。国家对商用密码产品的科研、生产、销售和使用实行专控管理”,“任何单位或者个人只能使用经国家密码管理机构认可的商用密码产品,不得使用自行研制的或者境外生产的密码产品”。因此,在选择 VPN 产品时,应选用经过国家密码管理局和公安部认证鉴定的产品。具体而言,合法的 VPN 设备制造商必须是国家密码管理局认定的“中国商用密码产品生产定点单位”,具备《国家商用密码产品销售许可证》。合法的 VPN 网关产品拥有国家密码管理局颁发的《商用密码产品技术鉴定证书》或产品型号证书,以及公安部颁发的《计算机信息系统安全专用产品销售许可证》。

如何寻找可靠和成熟的 VPN 产品?只需要看该产品的应用情况和成功案例即可。选购 VPN 产品,必须核实该产品在全国各地和各个行业都有广泛应用,核实是否有大规模和全国范围的成功案例,以证明产品的成熟性。

9.3.7 产品质量

VPN 专网是企业关键应用的运行平台，一旦出现故障，对用户的影响极大。因此，产品的质量是至关重要的。VPN 设备制造商的生产规范性是确保产品质量的有效保证之一。所以，考查 VPN 设备制造商是否通过 ISO 9000 质量管理体系认证是重要的。

另外，基于嵌入式的硬件平台相比于基于工控机平台的网关，长期运行稳定性提高 3～5 倍。通常，工控机很难确保在 3 年的连续运行期间不发生故障。所以，建议用户尽量选择采用嵌入式硬件平台的 VPN 安全网关。

9.3.8 厂商售后服务能力和水平

在 VPN 设备出现故障时，厂商或其经销商的服务速度和服务水平是至关重要的。为确保及时的现场服务，厂商应在全国各大城市都部署分支机构，应该有覆盖全国的服务网络。对经销商的技术服务人员，应该有专业的培训和认证。

此外，还应该重点关注厂商提供的各种增值服务，综合考虑在设备使用的生命周期内的综合投入和产出。

另外，厂商是否有较强的本地研发团队，来响应客户的二次开发需求，也是选择 VPN 品牌的重要因素。

总体来说，只有大型和专业的 VPN 厂商才能有效保证客户的投资。

习题 9

1. 构建企业级 VPN 网络时，应该从哪几个方面考虑购买何种 VPN 设备？
2. 国外主流的 VPN 设备有哪些？
3. 国内主流的 VPN 设备有哪些？

中英文对照

Access VPN	远程接入虚拟网
Authentication	身份认证技术
AH(Authentication Header)	认证头协议
ARP	地址解析协议
CAM	内容寻址器
CC(Common Criteria for Information Technology Security Evaluation)	信息技术安全性评价通用准则
CEM	公共测评方法
CHAP	挑战-握手验证协议
Compromised-Key Attack	盗取密钥攻击
Compulsory Tunnel	强制隧道
CPE-VPN	用户管理的 VPN
CTCPEC	加拿大可信计算机产品评估准则
Customer Devices	用户设备
Customer Edge Devices	用户边缘设备
Denial-of-Service Attack	拒绝服务攻击
DSL	数字用户线路
EAL(Evaluation Assurance Levels)	评估级别
ESP (Encapsulating Security Payload)	封装有效载荷协议
Extranet VPN	企业外部虚拟网
FC	信息技术安全联邦标准
FEC(Forwarding Equivalence Class)	转发等价类
GRE(Generic Routing Encapsulation)	通用路由封装协议
HMAC(Hash Message Authentication Codes)	Hash 信息验证码
HDLC	高级数据链路控制
HTTP(Hyper Text Transfer Protocol)	超文本传输协议
Intranet VPN	企业内部虚拟网
ISAKMP	Internet 安全联系和密钥管理协议
ISDN	综合业务数字网
ITSEC	信息技术安全评价标准
Key Management	密钥管理
L2F(Level 2 Forwarding Protocol)	第二层转发协议
L2TP	第二层隧道协议
Label	标记
Label Stack	标记栈
LAN	本地链路局域网

LDP(Label Distribute Protocol)	标记分发协议
LLC	逻辑链路控制
LS P(Label Switch Path)	标记交换路径
MAC	介质访问控制
Man-in-the-Middle Attack	中间人攻击
MIME	多功能 Internet 电子邮件扩充
MPLS(Multi-Protocol Label Switch)	协议标记交换
NAS (Network Access Server)	网络接入服务器
NCP	网络控制协议
Overlay Model	叠加模式
PAP	口令验证协议
Password-Based Attacks	盗用口令攻击
Peer Model	对等模式
PLMN	蜂窝移动通信网
PP	保护轮廓
PPP	点对点协议
PPTP	点对点隧道协议
PP-VPN	提供商实施的 VPN
PSTN	公众交换电话网
SA(Security Association)	安全关联
SAD(Security Association Database)	安全关联数据库
Site-to-Site intranet VPN	内联网 VPN
SLIP(Serial Line Internet Protocol)	串行线路互联协议
S/MIME	安全的多功能 Internet 电子邮件扩充
S-HTTP	安全超文本传输协议
SPD(Security Policy Database)	安全策略数据库
Service Provider (P) devices	服务运营商设备
Service Provider Edge (PE) devices	服务运营商边缘设备
SSID(Service Set Identifier)	服务集标识
SSH(Secure Shell Protocal)	安全外壳协议
SSL(Secure Sockets Layer)	安全套接字层协议
ST	安全规范
Strategic Implementation	策略执行
TCSEC	可信计算机系统评价准则
TOE	评估对象
Tunneling	隧道技术
Voluntary Tunnel	自愿隧道
VPN(Virtual Private Networks)	虚拟专用网
WAN	广域网

参考文献

[1] IETF Transport Layer Security(TLS)工作组[OL]. http://www. ietf. org/dyn/wg/charter/tls-charter. html,2009.

[2] FREIER A O,KARLTON P,KOCHER P C. The SSL Protocol Version 3. 0[EB/OL]. [2011-05-30]. http://tools. ietf. org/pdf/draft-ietf-tls-ssl-version3-00. pdf, Transport Layer Security Working Group,1996.

[3] IETF Secure Shell 工作组[OL]. http://tools. ietf. org/wg/secsh,2009.

[4] YLONEN T. ,F RFC4251: The Secure Shell(SSH)Protocol Architecture[EB/OL]. [2011-05-30]. ftp://ftp. rfc-editor. org/in-notes/rfc4251. txt,[2006-01-01].

[5] Transport Layer Security Working Group. Draft dependency graphs [EB/OL]. [2011-05-30]. http://www. fenron. com/~fenner/ietf/deps/viz/tls. pdf.

[6] OpenSSH Manual[OL]. http://www. openssh. org,2009.

[7] 关振胜. 公钥基础设施 PKI 及其应用[M]. 北京: 电子工业出版社,2008.

[8] H3C E126/E126A 以太网交换机操作手册[G]. 杭州: 杭州华三通信技术有限公司,2009.

[9] FRAHIM J,HUANG QIANG. SSL 与远程接入 VPN[M]. 王喆,罗进文,白帆,译. 北京: 人民邮电出版社,2009.

[10] SSH: UNIX Secure Shell Tool(PDFCN).

[11] 卢斌. 基于口令的网络安全认证协议研究[D]. 上海: 复旦大学,2008.

[12] 甘长华. 网络安全协议 SSH 的研究与实现[D]. 天津: 天津大学,2007.

[13] 陈国斌. 用 SSH 协议实现银行无线移动柜台[J]. 中国金融电脑,2004(10): 43-46.

[14] CNNIC. 中国互联网络发展状况统计报告(2012 年 1 月版)[OL]. 2012.

[15] ALLEN C,DIERKS T. [RFC 2246]: The TLS Protocol Version 1. 0,1999.

[16] DIERKS T,RESCORLA E. [RFC 4346]: Transport Layer Security(TLS) Protocol Version 1. 1,2006.

[17] DIERKS T,RESCORLA E. [RFC 5246]: The Transport Layer Security(TLS)Protocol Version 1. 2,2008.

[18] [RFC 4250] The Secure Shell(SSH)Protocol Assigned Numbers.

[19] [RFC 4251] The SecureShell(SSH)Protocol Architecture.

[20] [RFC 4252] The Secure Shell(SSH)Authentication Protocol.

[21] [RFC 4253] The Secure Shell(SSH)Transport Layer Protocol.

[22] [RFC 4254] The Secure Shell(SSH)Connection Protocol.

[23] [RFC 4256] Generic Message Exchange Authentication for the Secure Shell Protocol(SSH).

[24] [RFC 4335] The Secure Shell(SSH)Session Channel Break Extension.

[25] [RFC 4344] The Secure Shell(SSH)Transport Layer Encryption Modes.

[26] [RFC 4345] Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol.

[27] [RFC 4419] Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol.

[28] [RFC 4432] RSA Key Exchangefor the Secure Shell (SSH) Transport Layer Protocol.

[29] [RFC 4462] Generic Security Service Application Program Interface (GSS-API) Authentication

and Key Exchange for the Secure Shell (SSH) Protocol.
[30] SSL 协议Version 3.0 3/4/96[OL]. 隋立颖,译. http://www.snca.com.cn/Upload/200721216458844.doc.
[31] 寇晓蕤,王清贤. 网络安全协议——原理、结构与应用[M]. 北京:高等教育出版社,2008.
[32] SSH 技术白皮书[G]. 杭州华三通信技术有限公司,2010.
[33] SSL VPN 技术白皮书[G]. 杭州华三通信技术有限公司,2010.
[34] SSL 技术白皮书[G]. 杭州华三通信技术有限公司,2010.
[35] SSL 协议的安全性分析. [EB/OL]. [2011-05-30]. http://www.360doc.com/content/05/1221/14/2778_47552.shtml,2010.
[36] DAVIS C R. IPSec:VPN 的安全实施[M]. 周永彬,冯登国,徐震,等译. 北京:清华大学出版社,2002.
[37] 王春海,张晓莉,田浩. VPN 网络组建案例实录[M]. 北京:科学出版社,2008.

普通高等教育“十一五”国家级规划教材

计算机系列教材

主编：周立柱、王志英、李晓明

书名	作者	定价
计算机组织与体系结构(第 4 版)解题指南	白中英	19
计算机组织与体系结构(第 4 版 立体化教材)	白中英	43
计算机操作系统教程(第 3 版)	张尧学、史美林	25
计算机操作系统教程(第 3 版)习题解答与实验指导	张尧学	15
高档微机原理与技术	毛国君、方娟	21
计算机组成原理与汇编语言	易小琳 等	39
微型机原理与技术(第 2 版)	戴梅萼、史嘉权	33
微型机原理与技术——习题、实验和综合训练题集(第 2 版)	戴梅萼、史嘉权	18
编译原理	陈英 等	32
MPI 并行程序设计实例教程	张武生 等	39.5
计算机组成与设计	薛宏熙	36
数字逻辑设计	薛宏熙	33
计算机英语(第四版)	刘兆毓、郑家农	35
数据库系统设计与原理(第 2 版)	冯建华、周立柱	24
数据库专题训练	冯建华、周立柱	20
C/C++ 与数据结构(第 3 版)上册	王立柱	38
C/C++ 与数据结构(第 3 版)下册	王立柱	17
C/C++ 与数据结构(第 3 版)(上册)习题解答与实验指导	刘志红 等	18